UNITED STATES HOUSE COMMITTEE ON

FINANCIAL SERVICES

CHAIRMAN FRENCH HILL

JULY
2026

FIGHTING BACK: A POLICY FRAMEWORK FOR COMBATING THE RISE OF FINANCIAL FRAUD & SCAMS

Final Staff Report

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In December 2025, an Arkansas school district received wiring instructions to pay a contractor for ongoing construction work on a new high school campus.[1] An employee of the contractor notified the school district's director of finance via email of the outstanding amount and noted that someone would pick up the check in person.[2] That email, however, was moved from the director's inbox to her trash—likely after criminals gained access to the director's account.[3] The director then received an email from someone purporting to work at the contractor, but with the email address changed by a single letter.[4] That email indicated that no one was available to pick up a check, so the director should wire the outstanding amount—$3.2 million.[5] The director complied, and the criminals made off with millions.[6] Thankfully, the school district was able to recover the majority of the stolen funds, but many are less fortunate.[7] Take the case of Dennis Jones. The retired 82-year-old was befriended on social media by a woman named Jessie.[8] Mr. Jones and Jessie exchanged messages for months, ultimately developing a close relationship. At some point in that friendship, Jessie told Mr. Jones about an investment opportunity and urged Mr. Jones to participate. He complied, ultimately sending her his entire life savings. Then, one day, Jessie disappeared, leaving Mr. Jones with nothing. Mr. Jones's family sought to support him, but he ultimately took his own life.

These examples illustrate a growing crisis confronting Americans: financial fraud and scams. Criminals are increasingly targeting Americans and businesses, seeking to induce victims to turn over money or, in the case of fraud, illegally taking the funds without consent. While fraud schemes and scams have been around for decades, they are growing at an exponential rate both in terms of the number of victims and the monetary losses reported. Indeed, nearly 75 percent of Americans—hundreds of millions of people—have experienced some form of online scam or attack,[9] with an estimated 15 million Americans victimized in 2025 alone.[10] The Federal Trade Commission (FTC) received over 3 million fraud reports from customers and reported

---

[1] Anne Li, *Emails show how Pine Bluff School District was tricked into sending $3.2M to scammers posing as contractor*, ARK. DEMOCRAT GAZETTE (May 19, 2026), https://www.arkansasonline.com/news/2026/may/19/emails-show-how-pine-bluff-school-district-was/.
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] Rowdy Baribeau, *Pine Bluff School District scammed out of more than $3.2 million after cybersecurity hack*, KATV (Apr. 30, 2026), https://katv.com/news/local/pine-bluff-school-district-scammed-out-of-more-than-32-million-after-cybersecurity-hack.
[8] Teele Rebane & Ivan Watson, *Killed by a scam: A Father took his life after losing his savings to international criminal gangs. He's not the only one*, CNN (June 20, 2024), https://www.cnn.com/2024/06/17/asia/pig-butchering-scam-southeast-asia-dst-intl-hnk/index.html.
[9] Jeffrey Gottfried et al., *Online Scams and Attacks in America Today*, PEW RESEARCH CENTER (July 31, 2025), https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/.
[10] *See* UNITED STATES OF SCAMS: THE FINANCIAL AND EMOTIONAL FALLOUT, GALLUP & STOP SCAMS ALLIANCE (2026), *available at* https://news.gallup.com/poll/710984/scam-victims-report-billions-lost-harm-mental-health.aspx [hereinafter UNITED STATES OF SCAMS].

$15.9 billion in losses in 2025.[11] The reported losses represent a 28 percent increase from 2024[12] and a staggering 1,800 percent increase since 1997, when the FTC began tracking fraud and scam statistics. Moreover, when accounting for the vast majority of victims who do not report the fraud and scam attacks they have suffered, the $15.9 billion increases to an estimated $196 billion.[13]

No one is safe from these threats. Although elderly Americans have traditionally been the most vulnerable demographic due to their relative lack of familiarity with technology and the nature of fraud schemes and scams,[14] young people have become equally, or even more, susceptible to these schemes; in 2024, the success rate for fraud and scam attempts on Americans ages 20 to 29 was nearly twice the success rate against elderly Americans.[15] Likewise, education is no longer a foil against fraud and scams, with 37 percent of FTC fraud reports in 2025 submitted by Americans with a bachelor's degree or higher—roughly equivalent to their proportion of the population.[16] In sum, while the common American conception of fraud and scam victims may conjure images of an elderly person wiring their retirement savings to a "Nigerian Prince" tricked by nothing more than a poorly composed email, today's fraud and scam victims are Americans of all ages and educational backgrounds.

Fraudsters and scammers' success in diversifying their victim base is the byproduct of an increasingly complex, international shadow industry. Located primarily across Southeast Asia in nations such as Burma, Laos, and Cambodia, as many as 150 "scam centers"—industrial-scale scamming sweatshops—employ as many as 300,000 human-trafficked laborers to attack American consumers.[17] Many scam centers operate in Special Economic Zones created by the People's Republic of China, meaning host nations have minimal oversight of these operations.[18] Further, other criminal organizations, including Latin American drug cartels, have expanded their

---

[11] *Fraud Reports Tableau Public*, FED. TRADE COMM'N, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts (last visited July 2, 2026) [hereinafter FTC Fraud Reports Data]; *see also The Rising Global Scam Economy: Hearing Before J. Econ. Comm.*, 119th Cong. 2 (2026) [hereinafter *J. Econ. Comm. Hearing*] (prepared Testimony of Lois Greisman, Associate Director of the Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission).
[12] *Compare* FTC Fraud Reports Data, *supra* note 11 *with* FED. TRADE COMM'N, 2024 CONSUMER SENTINEL NETWORK DATA BOOK 6 (2025), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf [hereinafter 2024 FTC DATA BOOK].
[13] ASPEN INSTITUTE, A PERVASIVE THREAT: ANALYZING RECENT SURVEY DATA ON FRAUD AND SCAMS (2025) [hereinafter ASPEN INSTITUTE, A PERVASIVE THREAT].
[14] *Id.*
[15] 2024 FTC DATA BOOK, *supra* note 12, at 5.
[16] Press Release, U.S. Census Bureau, Census Bureau Releases New Educational Attainment Data, (Sep. 3, 2025) https://www.census.gov/newsroom/press-releases/2025/educational-attainment-data.html; ASPEN INSTITUTE, A PERVASIVE THREAT, *supra* note 13.
[17] Briefing with House of Representatives staff (notes on file with the Committee); UNITED NATIONS HUMAN RIGHTS COMMISSION, A WICKED PROBLEM SEEKING HUMAN RIGHTS-BASED SOLUTIONS TO TRAFFICKING INTO CYBER SCAM OPERATIONS IN SOUTHEAST ASIA (2026).
[18] U.S.-CHINA ECON. & SEC. REVIEW COMM'N, CHINA'S EXPLOITATION OF SCAM CENTERS IN SOUTHEAST ASIA (July 18, 2025), *available at* https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf [hereinafter U.S.-CHINA ECON. & SEC. REVIEW COMM'N, CHINA'S EXPLOITATION OF SCAM CENTERS].

activities to include fraud and scam operations.[19] These organizations find such activities to be a valuable hedge against inconsistent illicit drug revenue, often generating significant returns despite minimal fixed costs.[20] The professionalization and proliferation of these operations enable fraud and scams on an unprecedented scale.

Whether the perpetrators are Chinese syndicates, Latin American cartels, or third parties, fraud and scam payment schemes follow common patterns. Criminals contact victims digitally through a myriad of entry points, including social media platforms, dating apps, online marketplaces, text messages, robocalls, and emails.[21] Some schemes take the form of a single text or phone call impersonating the victim's financial institution or another trusted party.[22] These messages typically prompt the victim to provide a piece of sensitive financial information, such as a credit card or account number, which the criminal uses to gain illicit access to funds.[23] Other messages impersonate authority figures, financial professionals, investors, potential romantic partners, and others as the criminal attempts to establish rapport with the victim.[24] After gaining the victim's trust, the criminal requests funds, often under the pretense of a fabricated investment opportunity "guaranteed" to net the victim a large profit.[25] Upon receipt, the criminal will sever all contact and repeat the process with their next victim.[26]

These schemes have been enabled by rapid technological advancement. Encrypted messaging platforms offer features that protect anonymity, restrict law enforcement's ability to track down perpetrators, provide access to billions of potential victims, and act as online staging grounds for criminal groups.[27] Modern payment methods can facilitate the swift completion of

---

[19] Demian Bio, *Not Just Social Media: How Cartels are Exploiting the Cyber Space to Expand Their Activities*, LATIN TIMES (May 10, 2025), https://www.latintimes.com/not-just-social-media-how-cartels-are-exploiting-cyber-space-expand-their-activities-582732.

[20] *Id.*

[21] Jeff Horwitz & Angel Au-Yeung, *Meta Battles an "Epidemic of Scams" as Criminals Flood Instagram and Facebook*, WALL ST. J. (May 15, 2025), https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8?; Daniel Miller, *Amazon issues scam warning to millions of customers. What we know*, LIVENOW FOX (Nov. 26, 2025), https://www.livenowfox.com/news/amazon-scam-attack-warning-customers; Mary Cunningham, *Americans are getting 2.5 billion robocalls a month – the highest level in years*, CBS NEWS (Oct. 17, 2025), https://www.cbsnews.com/news/robocalls-on-the-rise-heres-why/; Press Release, Dept. of Treasury, U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia (Oct. 14, 2025), https://home.treasury.gov/news/press-releases/sb0278.

[22] Press Release, Fed. Trade Comm'n, New FTC Data Show Top Text Message Scams of 2024; Overall Losses to Text Scams Hit $470 Million (Apr. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/04/new-ftc-data-show-top-text-message-scams-2024-overall-losses-text-scams-hit-470-million.

[23] *Smishing: Package Tracking Text Scams*, U.S. POSTAL INSPECTION SERV., https://www.uspis.gov/news/scam-article/smishing-package-tracking-text-scams (last updated May 19, 2025).

[24] *Imposter Scams*, USA GOV, https://www.usa.gov/imposter-scams (last visited May 26, 2026); *FBI Warns Public to Beware of Scammers Impersonating FBI Agents and Other Government Officials*, FED. BUREAU OF INVESTIGATION (June 5, 2024), https://www.fbi.gov/contact-us/field-offices/portland/news/fbi-warns-public-to-beware-of-scammers-impersonating-fbi-agents-and-other-government-officials; *Stay Safe Online: Avoid Romance Scams*, U.S. SECRET SERV., https://www.secretservice.gov/investigations/romancescams (last visited May 26, 2026).

[25] INTERNET CRIME COMPLAINT CTR., FED. BUREAU OF INVESTIGATION, INTERNET CRIME REPORT (2025), *available at* https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf [hereinafter FBI 2025 INTERNET CRIME REPORT].

[26] U.S. GOV'T ACCOUNTABILITY OFF., GAO-25-107088, ACTIONS NEEDED TO IMPROVE COMPLAINT REPORTING, CONSUMER EDUCATION, AND FEDERAL COORDINATION TO COUNTER SCAMS (2025) [hereinafter GAO-25-107088].

[27] UNITED NATIONS HUMAN RIGHTS COMMISSION, *supra* note 17.

transactions and the equally swift removal of funds from the financial system before institutions or authorities can intervene.[28] And most recently, the increased utilization of artificial intelligence (AI) allows criminals to instantly generate emails, texts, voice messages, and videos nearly indistinguishable from legitimate communications.[29] These technologies further enhance the criminal capacity of large-scale scam centers, exponentially increasing the number of fraud and scam attempts while creating access to new vectors of scheme transmission.

Republican members of the House Committee on Financial Services (Committee) are determined to do what they can to address this growing threat. That is why the Committee has prioritized highlighting and addressing the crisis facing Americans. During the 119th Congress, the Committee has held multiple hearings and passed various pieces of legislation aimed at combating fraud and scams. Committee Republicans have also engaged with stakeholders across the public and private sectors to sound the alarm on the need to address this issue. The threat posed by fraud and scams impacts entities beyond a single industry or jurisdiction—it is a national challenge that requires an all-of-ecosystem approach. Committee Republicans' have focused on engaging with as many entities as possible that should be involved in fighting back against these crimes. The purpose of these efforts is to share takeaways with the broader community and highlight areas that need to be addressed for progress to be made in stemming the tide of fraud or scams.

From Committee Republicans' engagement, it is clear that, in the face of this overwhelming, increasingly complex threat, stakeholders, authorities, and the Administration are prioritizing solutions. Financial institutions are investing heavily in fraud detection and mitigation programs.[30] Telecommunications companies are rolling out features enabling consumers to block and report suspicious correspondence.[31] Social media and internet companies, while facing structural challenges, are working to combat these criminals.[32] Importantly, private sector actors as a whole are beginning to collaborate on anti-fraud and scam efforts through dedicated coalitions and partnerships.[33]

The Trump Administration has prioritized combatting these schemes as well, issuing several Executive Orders (EOs). These EOs direct agencies, such as the Department of the Treasury (Treasury Department) and the Financial Crimes Enforcement Network (FinCEN), to remove barriers to inter-agency collaboration on fraud and scam prevention, issue rules and notices combatting known perpetrators of fraud and scams, and take other actions.[34] Federal

---

[28] Djordje Djordjevic, *Telegram scams: how they work, what to watch for & how to protect yourself*, CYBERNEWS (May 27, 2026), https://cybernews.com/identity-theft-protection/telegram-scams/.
[29] NAT'L CONSUMER LEAGUE, DEEPFAKES, CHATBOTS, AND SCAMS: HOW AI IS FUELING FRAUD AND WHAT POLICYMAKERS MUST DO 2 (2025).
[30] U.S. GOV'T ACCOUNTABILITY OFF., GAO-24-107107, PAYMENT SCAMS: INFORMATION ON FINANCIAL INDUSTRY EFFORTS (2025).
[31] Briefings with Committee Republican staff (notes on file with the Committee).
[32] *See* News Release, Meta, Meta Partners with UK Banks to Combat Scams (Oct. 2, 2024), https://about.fb.com/news/2024/10/meta-partners-with-uk-banks-to-combat-scams/ [hereinafter Meta, Partners with UK Banks].
[33] *Id.*; ASPEN INSTITUTE, SCALING SCAM PREVENTION THROUGH SHARED INTELLIGENCE: MAPPING THE SOLUTIONS LANDSCAPE (2025), *available at* https://fraudtaskforce.aspeninstitute.org/mapping-scam-solutions [hereinafter ASPEN INSTITUTE, SCALING SCAM PREVENTION].
[34] Exec. Order No. 14,243, 90 Fed. Reg. 13,681 (2025); Exec. Order No. 14,249, 90 Fed. Reg. 14,011 (2025).

agencies are establishing task forces to combat these schemes, such as the Securities and Exchange Commission's (SEC) Cross-Border Task Force to Combat Fraud and the Financial Industry Regulatory Authority's Financial Intelligence Fusion Center.[35] Other federal authorities are promoting consumer outreach and education as a means to combat fraud and scams.[36] Locally, state attorneys general and state regulators are also working within their jurisdictions to combat fraud and scams. For example, through a partnership with the Texas Department of Licensing and Regulation and the Smith County District Attorney's Office, the state of Texas created a dedicated fusion center focused on combating financial crimes.[37]

Despite these stakeholders' efforts, there remains a substantial gap between criminal activity and effective enforcement. Committee Republicans believe that this gap could be reduced and eliminated through several measures, including but not limited to:

- Uniting agency initiatives under a single executive task force to permit more powerful, effective government initiatives.

- Integrating the over-a-dozen unique federal fraud and scam complaint centers to streamline intake, data collection, and, ultimately, action.[38]

- Establishing a cross-sector reporting framework to improve information sharing across public and private actors combating fraud and scams.

- Ensuring consistent taxonomy and terminology across public and private actors to permit a more accurate ascertainment of the scope of the problem and to generate higher quality issue reporting.

- Prioritizing investigation and prosecution of fraud and scam perpetrators to deter would-be criminals from such behavior.

---

[35] Press Release, Sec. & Exch. Comm'n, SEC Announces Formation of Cross-Border Task Force to Combat Fraud (Sep. 5, 2025), https://www.sec.gov/newsroom/press-releases/2025-113-sec-announces-formation-cross-border-task-force-combat-fraud; *FINRA Launches Financial Intelligence Fusion Center to Combat Cybersecurity and Fraud Threats*, BUSINESSWIRE (Mar. 31, 2026), https://www.businesswire.com/news/home/20260331051186/en/FINRA-Launches-Financial-Intelligence-Fusion-Center-to-Combat-Cybersecurity-and-Fraud-Threats.

[36] Briefings with Committee Republican Staff (notes on file with the Committee).

[37] Jacob Putman, *What is the Financial Crimes Intelligence Center?*, TX. DIST. & CTY ATTYS ASS'N (May-June 2023), https://www.tdcaa.com/journal/what-is-the-financial-crimes-intelligence-center/; Press Release, Off. of the Dist. Att'y of the County of San Diego, Elder Scam Prevention Campaign is Reaching Millions of County Residents in Effort to Reduce Devastating Losses to Seniors (Nov. 25, 2025), https://www.sdcda.org/content/office/newsroom/tempDownloads/389a9745-31ff-4037-b757-3e3636f9274e_Elder%20Scam%20Outreach%20District%20Attorney%20News%20Release%2011-25-25.pdf; Financial Crimes Intelligence Center at a Glance, TX. DEP'T OF LICENSING & REGULATION, https://www.tdlr.texas.gov/media/pdf/FCIC%20at%20a%20Glance.pdf.

[38] *See Report Fraud Waste and Abuse*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/services/report-fraud-waste-and-abuse (last visited June 29, 2026); *File a Complaint with Us*, INTERNET CRIME COMPLAINT CTR., https://www.ic3.gov/; *Report Fraud*, FED. TRADE COMM'N, https://reportfraud.ftc.gov/ (last visited June 29, 2026); *Fraud Prevention and Reporting – How to Report Fraud*, SOCIAL SEC. ADMIN., https://www.ssa.gov/fraud/ (last visited June 29, 2026).

- Maintaining agility and adaptability in fraud and scam prevention measures, which are essential to combating the issue; as technology creates novel fraud and scam opportunities, public and private actors must be ready to meet criminals at every turn.

- Removing regulatory barriers that may hinder financial institutions' and firms' ability to effectively prevent fraud and scams or mitigate financial losses for victims.

- Creating a national consumer education campaign on fraud and scams, akin to the "Smokey Bear" or "Click It or Ticket" campaigns, to spread awareness and help Americans recognize the signs of a fraud or scam before it is too late.[39]

- Finally, treating victims of fraud and scams with greater compassion, refuting the common perception that "they should have known better," which will help ameliorate the psychological impact of fraud and scams.[40]

COMMITTEE'S EFFORTS

Committee Republicans have prioritized addressing the rise in financial fraud and scams since the outset of the 119th Congress. Most Committee subcommittees have held a hearing specifically focused on the devastating impact fraud and scams have on Americans, as well as policy solutions to combat these crimes:

- On April 1, 2025, the Subcommittee on National Security, Illicit Finance, and International Financial Institutions held a hearing titled "Following the Money: Tools and Techniques to Combat Fraud."[41]

- On September 18, 2025, the Subcommittee on Oversight and Investigations held a hearing titled "Fraud in Focus: Exposing Financial Threats to American Families."[42]

- On March 5, 2026, the Subcommittee on Financial Institutions held a hearing titled "Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions."[43]

- On April 15, 2026, the Subcommittee on Capital Markets held a hearing titled "Safeguarding Main Street: Combating Fraud and Exploitation in our Capital Markets."[44]

---

[39] Briefings with Committee Republican staff (notes on file with the Committee).
[40] Luke Balcombe, *The Mental Health Impacts of Internet Scams*, INT. J. ENVIRON. RES. PUBLIC HEALTH (June 14, 2025), https://pmc.ncbi.nlm.nih.gov/articles/PMC12192844/.
[41] *Following the Money: Tools and Techniques to Combat Fraud: Hearing Before the Subcomm. on Nat'l Sec., Illicit Fin., & Int'l Fin. Insts. of the H. Comm. on Fin. Servs.*, 119th Cong. (2025).
[42] *Fraud in Focus: Exposing Financial Threats to American Families: Hearing Before the Subcomm. on Oversight & Investigations of the H. Comm. on Fin. Servs.*, 119th Cong. (2025).
[43] *Fighting Fraud on the Front Lines: Challenges and Opportunities for Financial Institutions: Hearing Before the Subcomm. on Fin. Insts. of the H. Comm. on Fin. Servs.*, 119th Cong. (2026).
[44] *Safeguarding Main Street: Combating Fraud and Exploitation in our Capital Markets: Hearing Before the Subcomm. on Cap. Mkts. of the H. Comm. on Fin. Servs.*, 119th Cong. (2026).

Across these four public hearings, the Committee has highlighted the exponential increase in financial fraud and scams, educated the public on how criminals are attacking all segments of the American population, unmasked the perpetrators of these crimes, and demonstrated the need for a whole-of-society approach to address these issues.

Other Committee hearings have also touched on these themes. For example, Members discussed fraud and scams as part of a May 2026 Subcommittee on National Security, Illicit Finance, and International Financial Institutions hearing that analyzed how to modernize the *Bank Secrecy Act* to address financial crimes in the 21st century.[45] Additionally, Members discussed digital asset fraud and the need for consumer protections during the Subcommittee on Digital Assets, Financial Technology, and Artificial Intelligence's February 2025 hearing on digital asset market structure legislation.[46] Members also discussed AI-enabled fraud, deepfake scams, and the importance of safeguarding consumers during a September 2025 Subcommittee on Digital Assets, Financial Technology, and Artificial Intelligence hearing on the use of AI in the financial system and a December 2025 Full Committee hearing on AI Innovation in Financial Services.[47]

Throughout the 119th Congress, Committee Republican staff have also engaged in extensive stakeholder outreach—meeting with experts, private sector entities, and public sector agencies. These stakeholders span industries and jurisdictions, including financial institutions, payment processors, credit card companies, financial technology firms, telecommunications firms, technology firms, and social media firms. Every stakeholder recognized the importance of combating fraud and scams but flagged that stilted cross-industry collaboration and other barriers continue to impact stakeholders' ability to fully address the problem.[48]

To foster better collaboration and information sharing, Committee Republicans hosted a series of roundtables, each of which spotlighted a different set of core stakeholders.

- On December 11, 2025, Committee Republicans hosted a roundtable featuring nine private sector companies from across industries. These entities highlighted innovative programs and processes deployed internally within their companies to prevent and mitigate fraud and scams.[49] Participants discussed the need for enhanced cross-industry collaboration and federal regulator engagement and prioritization.[50] More specifically, many private stakeholders noted they want to share information across industries to prevent financial fraud and scams but require clarity from federal regulators to avoid violating rules that prohibit the sharing of certain information.[51]

---

[45] *Modernizing the BSA for Financial Crime in the 21st Century: Hearing Before the Subcomm. on Nat'l Sec., Illicit Fin., & Int'l Fin. Insts. of the H. Comm. on Fin. Servs.*, 119th Cong. (2026).
[46] *A Golden Age of Digital Assets: Charting a Path Forward: Hearing Before the Subcomm. on Digit. Assets, Fin. Tech., & Artificial Intel. of the H. Comm. on Fin. Servs.,* 119th Cong. (2025).
[47] *Unlocking the Next Generation of AI in the U.S. Financial System for Consumers, Businesses, and Competitiveness: Hearing Before the Subcomm. on Digit. Assets, Fin. Tech., & Artificial Intel. of the H. Comm. on Fin. Servs.,* 119th Cong. (2025); *From Principles to Policy: Enabling 21st Century AI Innovation in Financial Services: Hearing Before the H. Comm. on Fin. Servs.*, 119th Cong. (2025).
[48] *See* Briefings with Committee Republican staff (notes on file with the Committee).
[49] *See* Committee Republican Member Roundtable (Dec. 11, 2025) (notes on file with the Committee).
[50] *See id.*
[51] *See id.*

The participants pointed to the need for federal regulators to create opportunities, or regulatory safe harbors, to enhance information and data-sharing.[52]

- On April 15, 2026, Committee Republicans hosted a roundtable attended by eight representatives from local, state, and federal law enforcement entities. All participants emphasized the need for increased public and private collaboration.[53] Participants acknowledged the need for private companies to introduce greater friction in the payment process, the use of multi-factor authentication to protect account access, and consumer education.[54] However, participants also highlighted the importance of state-level leadership on this issue and the need for increased prosecution of these crimes.[55] Importantly, all participants were eager to continue conversations and collaboration following the roundtable.[56]

- On May 21, 2026, Committee Republicans hosted a roundtable attended by officials from five federal regulatory agencies, all of which play an important role in addressing fraud and scams. Each of the participating agencies stressed that they are doing the best they can to combat fraud and scams with the resources they have.[57] They agreed, however, that better consumer education and information sharing across foreign and domestic governments, as well as with private sector, will be necessary to combat fraud and scams and to protect Americans.[58]

KEY FINDINGS & RECOMMENDATIONS

Key Findings

1. Criminals are increasingly targeting and bankrupting Americans via financial fraud and scams. The FTC estimated that, in 2025, Americans reported losing nearly $16 billion—the highest figure ever reported.

2. The true monetary loss attributable to fraud and scams is likely closer to $200 billion, considering most fraud and scam victims fail to report these crimes. A multitude of reasons exist for the lack of reporting, including (a) a sense of shame for having been victimized, (b) confusion over where to report, and (c) disillusionment over law enforcement's prioritization of the claim.

3. Fraud and scams are not merely growing in volume. They are growing in sophistication, speed, and psychological precision. AI and other advanced technology have given criminal organizations the ability to generate personalized, culturally calibrated, grammatically flawless communications at mass scale; to clone the voices of loved ones that are indistinguishable from

---

[52] *See id.*
[53] *See* Committee Republican Member Roundtable (Apr. 15, 2026) (notes on file with the Committee).
[54] *See id.*
[55] *See id.*
[56] *See id.*
[57] *See* Committee Republican Member Roundtable (May 21, 2026) (notes on file with the Committee).
[58] *See id.*

real distress calls; and to create deepfake videos convincing enough to authorize substantial wire transfers from the finance departments of major corporations.

4. Given these advents, no Americans have been spared. According to one report, nearly three-quarters of the American population have experienced some form of online scam or attack.[59] Criminals are targeting Americans regardless of race, demographic, geographic location, education level, or income level.

5. Increasingly, the criminals perpetrating fraud and scams against Americans are sophisticated transnational criminal organizations, largely emanating from "scam centers" in Southeast Asia. Many of the individuals employed in these efforts are victims in their own right, having been lured and trafficked to the compounds and forced against their will by threat of violence to carry out criminal schemes. U.S. geopolitical rivals and adversaries, including those in China, Russia, and North Korea, are also working to leverage these schemes to harm Americans and undermine U.S. interests.

6. Although modern fraud and scams end with the transfer of money through a financial institution, they often start through other modalities, including social media, dating websites, phone calls, email, and messaging systems. In other words, various industries are implicated in the lifecycle of a scam.

7. Regarding where to report, the answer varies depending on the type of fraud and scam involved. There is no single reporting mechanism. At the federal level alone, there are no fewer than a dozen distinct agencies and portals that receive fraud or scam complaints, each with its own jurisdiction, intake form, and purpose. Beyond the federal level, local and state law enforcement, including many state attorneys general offices, maintain their own systems for reporting fraud and scams. This often results in victims feeling confused and overwhelmed, with many opting not to report at all.

8. Financial fraud and scams are of such a magnitude and complexity that no one person, company, or agency can tackle the problem alone. Given the number of sectors involved, public and private entities often have only a piece of the information needed to prevent fraud and scams and hold the bad actors accountable.

9. Stakeholders across the financial services, tech, and telecommunications industries are taking action to combat fraud and scams. As these crimes grow in scale and sophistication, companies within the industries most impacted have worked to develop layered defenses designed to slow, detect, and block fraudsters. Financial institutions, financial technology companies, telecommunications providers, and social media companies are each

[59] Gottfried et al., *supra* note 9.

deploying a combination of behavioral technology and regulatory compliance measures.

10. Companies are also increasingly establishing private cross-industry coalitions dedicated to sharing intelligence, pooling resources, and coordinating responses across sectors that have traditionally operated in silos. The federal government is also establishing inter- and intra-agency working groups. Nevertheless, legal and regulatory risks prohibit or dissuade real-time information sharing across industries.

11. Since the start of 2026, the Trump Administration has pursued one of the most ambitious federal anti-fraud agendas in recent history, issuing major EOs, announcing a new Department of Justice (DOJ) enforcement division, and establishing a White House-led task force. Together, these actions represent a significant restructuring of how the federal government coordinates its response to cybercrime, online scams, and fraudulent exploitation of American taxpayers.

12. State and local entities are also working to address fraud and scams. For example, many state attorneys general have launched consumer education campaigns and used their legal jurisdiction to hold bad actors accountable. Similarly, in Texas, the state government established a specialized financial crime center to coordinate law enforcement efforts across the state.

13. Both public and private sectors are investing in consumer education campaigns. Stakeholders with whom Committee staff engaged highlighted alerts, notices, reminders, mailings, webinars, and other ways in which they communicate with consumers about fraud and scams. However, these public awareness campaigns are currently independent and fragmented, with no coordinating authority and no consistent national message.

14. Despite increasing efforts to address financial fraud and scams, no entity has established a formalized plan for bringing together stakeholders to coordinate efforts. For example, no government entity is charged with harnessing and amplifying federal resources and efforts that are currently occurring. The existing fragmentation risks diminishing the efficiency and effectiveness of ongoing efforts.

15. Certain legal regimes distinguish between an unauthorized “fraud” and authorized “scams.” However, many agencies—and victims—do not recognize this distinction. The absence of a uniform, cross industry definition of what constitutes a “fraud” versus a “scam” creates inconsistent reporting, complicates liability determinations, and fosters an inability to accurately quantify the full scope of harms to consumers.

16. The sheer volume of fraud reports requires law enforcement to prioritize the largest and most widespread cases of fraud. However, according to officials, every U.S. Attorney Office has a different intake and threshold number, or loss amount, necessary to initiate an investigation.

Recommendations

1. **The federal government should establish coordinated, interagency Task Forces to help combat fraud and scams.** One consistent theme throughout Committee Republicans' work is the need for a coordinated all-of-government approach. Various pieces of legislation exist calling for new or existing government task forces to address fraud and scams. To sufficiently address these crimes, there must be cohesion and formality to the government's efforts. This coordinated effort will serve as a signal to adversaries that preventing and prohibiting fraud and scams is a national priority. Any task force should focus not only on engaging across the Administration, but also with Congress, private industry partners, foreign counterparts, and the American public to identify, prevent, and disrupt criminal schemes.

2. **The federal government should impose targeted sanctions against scam operators and their foreign government facilitators.** Scam centers have flourished often because the criminals behind them enjoy political protection or, at least, governmental ignorance. With many of these criminals now operating from abroad, the Executive Branch must coordinate with international partners to do more to eliminate these criminal schemes. To that end, the Executive Branch must use its authorities to pressure foreign and multinational counterparts to address this issue. In addition to sanctions, this could include visa restrictions, anti-money laundering authorities, and diplomatic engagement.

3. **The federal government should harmonize data collection and reporting systems to create a cohesive system through which individuals and entities can receive and disseminate reports of fraud and scams.** A cohesive reporting system should aid victims in quickly and easily reporting instances of fraud and scams, as well as provide a comprehensive dataset to inform law enforcement, regulators, and the American public about the scope of fraud and scams, including type, dollar loss amount, payment method, and other data fields, as appropriate.

4. **Law enforcement entities must better prioritize combating fraud and scams, including prosecuting criminals and publicizing successful lawsuits.** Law enforcement should explore methods for aggregating reported losses since criminals often use common schemes across victims. Congress must also ensure that law enforcement agencies have the tools and capabilities to address these crimes. As part of this effort, Congress should pass the *Guarding Unprotected Retirees from Deception (GUARD) Act*, which would allow state and local law enforcement to utilize funding from certain existing federal law enforcement grant programs to facilitate the retention and training of personnel and other enforcement activities associated with the countering

of general financial fraud, elder fraud, and pig butchering. Finally, law enforcement must do a better job of publicizing their wins—demonstrating to criminals the consequences of their actions and showing Americans that law enforcement is there to support them.

5. **Platforms that host advertisements—such as social media and technology companies—should verify advertisers and promptly investigate and remove advertisements reported as fraudulent.** Congress should consider proposed legislation, such as the *Safeguarding Consumers from Advertising Misconduct (SCAM) Act*, which would impose legal penalties on tech platforms accountable for or facilitating fraudulent and deceptive online advertisements. To the extent entities receive reports of fraudulent or scam content, those entities should promptly investigate, disable, and remove both the content and the entities behind it.

6. **The Federal Communications Commission (FCC) and FTC should consider requiring companies within their jurisdiction to enhance monitoring and authentication and to remove scam messages and the actors behind them.** Entities that receive reports of fraudulent or scam activity should promptly work to investigate, block, or otherwise intervene to reduce consumer losses.

7. **Congress and federal financial regulators should remove statutory and regulatory barriers, as appropriate, that prevent financial institutions and other industries from collaboratively combating fraud and scams.** Regulatory uncertainty can make it more difficult for financial institutions to collaborate with each other and other industries in their efforts to identify red flags that are critical in combating fraud and scams before they result in losses for everyday Americans. Regulators should look at removing barriers to information sharing to ensure robust collaboration. Furthermore, financial institutions and firms are often required to make funds available in specified timeframes with regulatory exceptions. To aid this effort, Congress should pass H.R. 9331, the *Strengthening Transaction Oversight and Preventing (STOP) Payments Fraud Act of 2026*. This bill amends the *Expedited Funds Availability Act* (EFAA) to permit the Federal Reserve Board and Consumer Financial Protection Bureau to remove Treasury and cashiers' checks from expedited funds availability requirements, establish an explicit fraud-related exception allowing financial institutions to slow down the availability of funds when fraud and scams are suspected, and permit exception holds for funds received through wire transfers. This provides targeted flexibility to combat fraud, while preserving timely access to legitimate funds.

8. **Other federal regulators should also remove regulatory barriers that prevent entities over which they have jurisdiction from working collaboratively to combat fraud and scams.** In June 2026, FinCEN issued guidance clarifying that covered financial institutions can share information relating to certain fraud and scam crimes. Regulators that oversee other

important industries—particularly the FCC and FTC—should issue similar guidance clarifying under what circumstances regulated entities are able to share information related to suspected fraud and scams with one another.

9. **States should consider establishing specialized financial crime centers.** Some states have created specialized law enforcement entities focused on addressing financial crime, such as the Texas Financial Crimes Intelligence Center. These groups have proven successful in identifying, investigating, and prosecuting criminal networks within the state. Such structures could be leveraged by other states to further combat these crimes.

10. **Private sector entities must implement, maintain, and continually strengthen anti-fraud and anti-scam policies.** While the federal government prioritizes combating fraud and scams, the private sector must also work to implement anti-fraud and anti-scam policies. For those with existing programs, it is imperative that those companies continually review and update their programs to ensure they account for the latest trends and developments. For those that do not yet have existing programs, it is imperative that they implement programs quickly and effectively. Criminals are constantly evolving their tactics, so too must defenses be updated to ensure they are effective and efficient.

11. **Federal government agencies, law enforcement, and private sector companies must embrace AI tools and cutting-edge technology to identify and investigate fraud and scams.** Criminals are increasingly adopting AI and other cutting-edge technologies to perpetuate fraud and crimes. The counter to this is ensuring that those empowered to prevent and respond to fraud and scams—namely public and private sector entities—deploy the same tools. To that end, Congress should pass H.R. 8671, the *Bank Fraud Technology Advancement Act of 2026*, which authorizes federal financial regulators to establish a pilot program for community financial institutions, expanding access to innovative and emerging fraud-prevention technologies. This legislation supports financial institutions in leveraging the same advanced technologies to strengthen their defenses against these evolving threats.

12. **Congress and federal regulators must better understand financial institutions' use of advanced technologies to detect, prevent, and combat financial fraud and scams.** As public and private sector entities continue to adopt innovative tools to address fraud and scams, it is imperative that Congress and federal regulators understand the use and effectiveness of such tools. By improving insight into the effectiveness of these technologies, Congress and regulators can help identify both successful practices and any regulatory or operational barriers that may limit their adoption. To this end, Congress should pass H.R. 2152, the *Artificial intelligence Practices, Logistics, Actions, and Necessities (AI PLAN Act)*, which directs the Treasury Department, the Department of Homeland Security, and the Department of Commerce to jointly submit a report assessing the national and economic

security risks posed by the use of AI in financial crimes, including fraud and scams. As part of this, the agencies would also evaluate specific threats and identify the additional resources federal agencies need to address these risks effectively. Following submission of the report, the agencies would be required to provide recommendations for legislative action, as well as best practices for both public and private sector entities to mitigate and respond to these emerging threats.

13. **Congress and the President should address the growing use of digital assets in fraud and scams, while fostering the legitimate uses of such assets.** To achieve this, Congress should pass H.R. 2384, the *Financial Technology Protection Act (FTPA)*, which would establish a working group between government and the digital asset ecosystem, research transactions related to terrorism and illicit financial technology, and implement actions to prevent money laundering and counter illicit financing in the United States. Similarly, Congress should pass H.R. 5877, the *Combatting Money Laundering in Cyber Crime Act of 2025*, which strengthens the authorities for the U.S. Secret Service to investigate various crimes related to digital asset transactions and to counter transnational cyber-criminal activity.

14. **Congress should provide regulators with authorities to address fraud, market manipulation, and illicit finance in digital asset markets and strengthen consumer protections.** The *CLARITY Act* would establish a comprehensive regulatory framework for digital asset markets and strengthen anti-money laundering (AML) and compliance requirements for digital asset intermediaries. The bill also extends the SEC's and Commodity Futures Trading Commission's anti-fraud authorities to digital asset markets, directs federal agencies to study blockchain-related payment fraud, and ensures investors and consumers transacting in digital assets are protected under federal anti-fraud laws. By closing regulatory gaps and creating clear rules of the road, the legislation would enhance regulators' ability to detect and deter fraud, market manipulation, and illicit finance while improving consumer and investor protections. The Executive Branch should also fully implement the *Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act*, which was enacted in July 2025. The *GENIUS Act* helps prevent fraud and illicit activity in the payment stablecoin market by establishing reserve, disclosure, supervision, and AML requirements for payment stablecoin issuers, thereby strengthening consumer protections and market integrity.

15. **Congress should permit financial firms to implement delays in the redemption period where indicators of fraud and scams exist.** The efforts would be especially helpful to protect seniors and other potential victims. For example, Congress should pass H.R. 2478, the *Financial Exploitation Prevention Act*. The bill delays the redemption period of any redeemable security if there is reasonable believe that such redemption was requested through the financial exploitation of a security holder who is a senior or an individual unable to protect their own interests. It also requires the SEC to

provide Congress with recommendations for legislative and regulatory changes on how to combat financial exploitation of seniors and vulnerable adults.

16. **The federal government should create a unified, national public awareness campaign related to fraud and scams.** Metrics should also be established to measure the effectiveness of the campaign and engagement therewith. This campaign should be a public-private partnership and include participants from the financial services, telecommunications, and social media industries, as well as law enforcement.

INTRODUCTION

When skimming the headlines of any news outlet, one is nearly guaranteed to see a story detailing a victim of fraud or a scam. Many of these stories are dramatic: in 2024, an Illinois widower lost nearly $1 million in a financial grooming scheme[60]; a Bay Area man lost $1 million after responding to a wrong-number text[61]; and a 75-year-old Los Angeles small business owner lost his life savings to a fake digital asset platform[62]. These stories, however, are not anomalies. They are the daily results of a global criminal industry that has professionalized deception at scale—an industry that, based on reported losses, took nearly $16 billion from Americans in 2025 alone, per data maintained by the Federal Trade Commission (FTC). The actual toll of losses to fraud and scams is estimated to be closer to $200 billion when accounting for the vast majority of victims who never report.

The scale and impact of the problem are difficult to overstate. Approximately 75 percent of Americans have experienced some form of online scam or attack.[63] The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) crossed one million complaints for the first time in 2025, with total reported losses of $20.8 billion—a 26 percent increase from the prior year.[64] Fraud is not only growing in volume, but also in sophistication, speed, and psychological precision. Artificial intelligence (AI) and other advanced technologies have given criminal organizations the ability to generate personalized, culturally calibrated, grammatically flawless communications at mass scale. For example, one could clone the voices of loved ones that are indistinguishable from real distress calls and create deepfake videos convincing enough to authorize substantial wire transfers from the finance departments of major corporations.

The entities behind this epidemic are not solely lone fraudsters working from laptop computers. They are increasingly transnational organized crime syndicates, many of which operate from fortified compounds in Southeast Asia.[65] Although it is easy to think of these individuals as criminals, many of those perpetrating fraud schemes and scams are trafficked workers being held against their will, stripped of their personal documents, and forced under threat of violence to spend twelve-hour shifts manipulating victims across time zones.

Private sector companies and public agencies acknowledge the threat posed by fraud and scams and are independently and collectively taking action to address these threats. Yet, despite these efforts, the impact of fraud and scams has continued to grow. The status quo is simply unacceptable. The fraud epidemic is an active, worsening crisis—one that destroys financial

---

[60] Jason Knowles & Ann Pistone, *Lombard Woman Loses Nearly $1 Million Life Savings in 'Pig Butchering' Scam*, ABC7 (Sep. 4, 2024), https://abc7chicago.com/post/lombard-woman-loses-1-million-life-savings-pig-butchering-scam-forced-sell-home-belongings/15267382/.
[61] Stephanie Sierra & Renee Koury, *Bay Area Widower Lured to Fake Romance, Loses $1 million in 'Wrong Number' Crypto Scam*, ABC7 (Oct. 30, 2025), https://abc7news.com/post/pig-butchering-wrong-number-text-causes-bay-area-man-lose-1-million-crypto-investment-romance-scam/18086833/.
[62] Bobby Allyn, *He Lost $340,000 to a Crypto Scam. Such Cases are on the Rise*, NPR (June 25, 2023), https://www.npr.org/2023/06/25/1180256165/crypto-scam-senior-victims-spirebit.
[63] Gottfried et al., *supra* note 9.
[64] FBI 2025 INTERNET CRIME REPORT, *supra* note 25.
[65] UN News, *Crushing Scam Farms, Southeast Asia's 'Criminal Service Providers'*, U.N. Off. on Drugs and Crime (July 2024), https://www.unodc.org/unodc/frontpage/2024/July/crushing-scam-farms--southeast-asias-criminal-service-providers.html.

security, devastates mental health, enables human trafficking, funds organized crime, and, in a growing number of documented cases, ends lives. As House Committee on Financial Services (Committee) Chairman French Hill noted in one of the Committee's hearings, "[f]raud and scams are not a new challenge, but the scale and complexity of the problem . . . are increasing rapidly, imposing a greater cost on both American families and the financial services arena."[66] This crisis demands the full, coordinated, sustained attention of every institution with any capacity to address it.

DEFINING FINANCIAL FRAUD AND SCAMS

Financial fraud and scams represent a significant and growing threat to the U.S. financial ecosystem.[67] Although both fraud and scams are devastating to consumers, there is a notable and legally consequential distinction between the two. Financial fraud is "when a customer's financial account is used *without their authorization*."[68] Financial scams "occur *with a customer's authorization*, but under false pretenses."[69] Various stakeholders stressed that the terms can be thought of synonymously given that victims do not distinguish.[70] However, unauthorized financial fraud and authorized financial scams trigger separate regulatory and legal obligations, particularly for financial institutions.[71]

The *Electronic Fund Transfer Act* (EFTA), enacted in 1978 and implemented through Regulation E (Reg E), provides the foundational legal framework governing consumer electronic payment transactions.[72] EFTA, and by extension Reg E, establishes protections against fraud—or the "unauthorized electronic fund transfers (EFTs)"[73]—including when fraudulent payments are made through "debit card transactions, electronic withdrawals, transfers, and deposits through automated teller machines (ATMs), automated clearinghouse systems (ACH), and remote banking programs."[74] An EFT is considered fraudulent under the EFTA when it is "initiated by a person other than the consumer with actual authority to initiate the transfer and from which the consumer receives no benefit."[75]

Under the EFTA and Reg E, financial institutions bear significant liability for fraudulent, unauthorized transactions, and importantly, consumer negligence cannot be used as the basis for

[66] *Fighting Fraud on the Front Lines*, *supra* note 43 (statement of Rep. Hill, Chairman, H. Comm. on Financial Servs.).
[67] *Payments Fraud Landscape: A Complex, Interconnected Web*, FED. RESV., https://fedpaymentsimprovement.org/news/blog/todays-payments-fraud-landscape-a-complex-interconnected-web/ (last visited May 26, 2026).
[68] Tara Payne, *Fraud vs. Scams: What's the Difference?*, BANK POLICY INST. (Feb. 4, 2026), https://bpi.com/fraud-vs-scams-whats-the-difference/ (emphasis added).
[69] *Id.*
[70] *See, e.g.*, Committee Republican Member Roundtable (May 21, 2026) (notes on file with the Committee).
[71] GAO-24-107107, *supra* note 30.
[72] 15 U.S.C. § 1693-1693r; 12 C.F.R. Part 1005 (2023); *Electronic Funds Transfer Act*, CORNELL LAW SCHOOL, https://www.law.cornell.edu/wex/electronic_funds_transfer_act (last visited May 26, 2026).
[73] *Electronic Funds Transfer Act*, CORNELL LAW SCHOOL, *supra* note 72.
[74] *Id.*
[75] *Id.*

imposing greater liability on the consumer.[76] As a general matter, financial institutions will compensate the victim for unauthorized transactions and bear the costs of the fraud themselves.[77] Consumer liability is carefully tiered based on the speed of reporting. If a consumer reports an unauthorized transfer within two business days of learning of the loss or theft,[78] their maximum liability is $50; reporting within sixty days caps liability at $500.[79] Reg E also provides the same protection to unauthorized debit card payments and ATM transactions,[80] and similar principles apply to credit cards under Regulation Z.[81] These protections reflect a Congressional determination that, when unauthorized fraud occurs, the financial institution should bear the primary burden of financial loss.[82]

Conversely, in the context of scams, traditional financial institutions are under no legal obligation to repay consumers given that the payments are authorized remittances.[83] This is commonly referred to as an authorized push payment (APP).[84] APP scams have grown in recent years alongside the integration of real-time payment platforms.[85] Congress recognized the distinction is important to defend against a moral hazard problem. Excluding liability in the event of *authorized* payments preserved consumer accountability and discouraged bad behavior.[86] Eliminating such accountability would remove consumers' incentive to scrutinize payment requests, protect account credentials, or exercise caution when responding to unsolicited contacts.[87] It would also increase instances of first-party fraud where bank customers themselves coordinate with criminals to defraud their financial institution and split the profits.[88] This could, in turn, cause further increases in scams, as criminals know that banks will foot the bill for consumers.[89]

---

[76] 15 U.S.C. § 1693g (2023); 12 C.F.R. § 1005.6 (2023); *See also id.* pt. 1005, supp. I, cmt. 6(b)-2 (stating "negligence by the consumer cannot be used as the basis for imposing greater liability than is permissible under Regulation E."), *available at* https://www.consumerfinance.gov/rules-policy/regulations/1005/interp-6/.

[77] 12 C.F.R. § 1005.2 (defining "unauthorized electronic fund transfer" as a transfer initiated without actual authority where the consumer receives no benefit); 12 C.F.R. § 1005.6(b) (2023) (limiting consumer liability for such transfers and placing the remaining financial burden on the institution).

[78] *See* 12 C.F.R. § 1005.6, supp. I, cmt. 6(1) ("The fact that a consumer has received a periodic statement that reflects unauthorized transfers may be a factor in determining whether the consumer had knowledge of the loss or theft but cannot be deemed to represent conclusive evidence that the consumer had such knowledge.").

[79] 15 U.S.C. § 1693g(a) (reporting after sixty days could result in full consumer liability).

[80] 12 C.F.R. § 1005.2.

[81] 12 C.F.R. § 1026.12.

[82] 15 U.S.C. §§ 1693b, 1693g; 12 C.F.R. § 1005.6.

[83] 12 C.F.R. §§ 1005.2(m), 1005.11. *See also id.* pt. 1005, supp. I, cmt. 2(m)-1 (explaining that an unauthorized transfer must be initiated by a person other than the consumer, thereby excluding transactions where the consumer personally executes a transfer due to fraudulent inducement).

[84] Simon Taylor, *Fraud vs Scam: What's the Difference? Prevent Fraud in Your Business*, SARDINE (Feb. 6, 2024), https://www.sardine.ai/blog/fraud-vs-scam.

[85] Chris Colson, *Addressing Authorized Push Payment Scams in the US*, FED. RESV. BANK OF ATLANTA (Sep. 23, 2024), https://www.atlantafed.org/research-and-data/publications/take-on-payments/2024/09/23/addressing-authorized-push-payment-fraud-in-us.

[86] 15 U.S.C. § 1693g.

[87] Andrew Kliewer, *The P2P Fraud Conundrum*, THE REGULATORY REVIEW (Sep. 1, 2022), https://www.theregreview.org/2022/09/01/kliewer-the-p2p-fraud-conundrum/.

[88] *Id.*

[89] Letter from American Bankers Association et al., to Richard Blumenthal et al., Senator (Aug. 28, 2024), *available at* https://www.icba.org/w/joint-letter-on-protecting-consumers-from-payment-scams-act.

Provided the scammed funds remain in the financial system, in a way that U.S. banks can access, financial institutions can attempt to hold or reclaim funds.[90] Unfortunately, by the time the scam is reported, it is frequently too late in the process for the bank to place a hold on transactions, limiting the ability for either the bank or consumer to reclaim funds.[91] Victims of scams are often left with few avenues for recourse and frequently are disappointed in the financial institutions, believing their financial institution should have done more to prevent the scam or reclaim the funds.[92] As a result, most financial institutions view scams as a substantial reputational risk and are working to implement policies, tools, and education to combat and prevent scams—all of which are described further below.[93]

THE LIFECYCLE OF FRAUD AND SCAMS

Although there are many different types of fraud and scams, most follow one of two primary lifecycles depending on whether the victim is directly contacted. In some instances, fraud and scams are completed without the perpetrator making direct contact with the victim.[94] These schemes generally involve fraudsters or scammers tricking the victim into giving their personal or financial information, then maliciously using this information, or the access it provides, to steal funds, property, or other items of value.[95] This lifecycle is typically seen with phishing, and certain types of online shopping, pop-ups, advanced fees, and mail and check fraud.[96]

Many of the most common and profitable types of fraud and scams, by contrast, involve direct communication between the fraudster or scammer and victim.[97] Although modern fraud and scams end with a transmittance of money through a financial institution, they start through other modalities, including:

- Social media platforms and dating websites;[98]
- Online marketplaces or messaging applications where scammers can operate anonymously and at scale;[99]
- Text messages, robocalls, and spoofed caller IDs facilitated by telecommunications providers;[100] and

---

[90] Ellie Farrier, *Do banks Refund Scammed Money*, LIFELOCK (May 13, 2026), https://lifelock.norton.com/learn/fraud/do-banks-refund-scammed-money.
[91] *Id.*
[92] *Id.*
[93] *The Trust Factor: Turning Fraud Challenges into Customer Loyalty Opportunities for Financial Institutions*, AM. BANKERS ASSOC. (June 3, 2025), https://www.aba.com/news-research/analysis-guides/the-trust-factor.
[94] *See generally Common Fraud and Scams*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams (last visited May 26, 2025).
[95] *Id.*
[96] *Id.*
[97] GAO-25-107088, *supra* note 26, at 1-2.
[98] Horwitz & Au-Yeung, *supra* note 21.
[99] Miller, *supra* note 21.
[100] Cunningham, *supra* note 21.

- Phishing emails or malware attacks.[101]

The perpetrators build and leverage personal connections with victims to increase the victims' willingness to make payments.[102] While building this relationship, fraudsters and scammers will frequently move their communications with the victim to a different, less monitored platform, such as WhatsApp, Telegram, or WeChat.[103] Finally, the fraudster or scammer will request or demand payment from the victim and abscond with any provided funds.[104]

The exact process fraudsters and scammers follow in their schemes is highly dependent on the method used to communicate with the victim.[105] Moreover, fraudsters and scammers will tailor their outreach methods based on the type of fraud or scam they seek to commit.[106] Generally, high-volume contact methods, such as email, phone calls, and text messages consistently represent the most common method of initial outreach but have lower success rates and average losses.[107] Conversely, social media tends to be the initial contact method with the highest success rate and largest average financial loss for victims but is less conducive to voluminous outreach.[108]

A. Fraud and Scams Through Social Media Accounts and Dating Profiles

Social media and online dating profiles are commonly employed by fraudsters and scammers to make initial contact with their victims.[109] Fraudsters and scammers create accounts on these services with fake information—increasingly leveraging AI-generated information or information on the dark web—and send friend requests, messages, or "likes" to a victim.[110] From that point, the fraudster or scammer will begin building their relationship with the victim, laying the groundwork for their scheme. The scammer will eventually request money from their victim, often for fake, urgent reasons.[111]

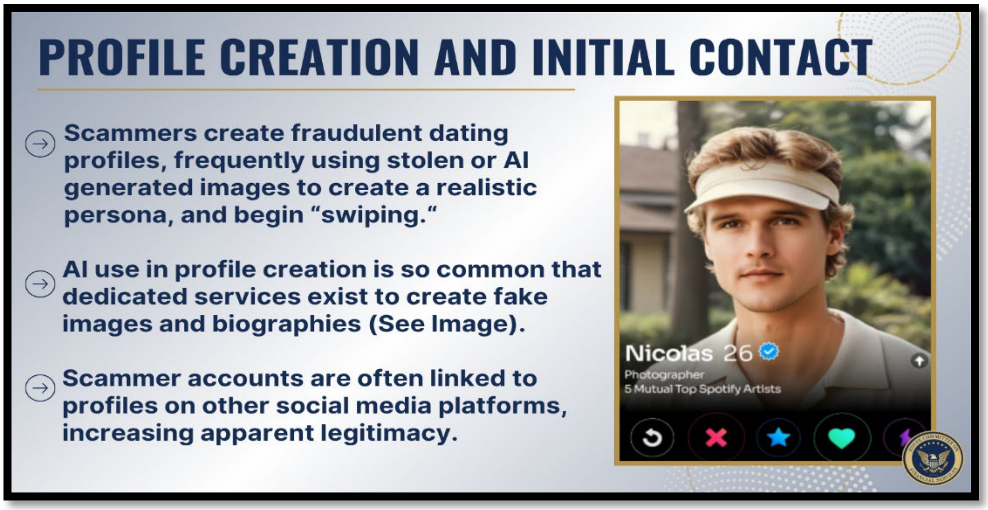
Different types of fraud and scams can be initiated through accounts on social media and dating applications, and these fraud and scam efforts can vary greatly in complexity and depth.[112] Regardless, each type of scheme still revolves around initiating contact, building trust, escalating the situation, and finally, payment.[113] In 2025, 11 percent of reported fraud and scam attempts

---

[101] *See generally Common Fraud and Scams*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams (last visited May 26, 2025).
[102] GAO-25-107088, *supra* note 26, at 9.
[103] *What is a Pig Butchering Scam?*, ATT'Y GEN. OF THE STATE OF NEW YORK, https://ag.ny.gov/publications/pig-butchering-scams (last visited June 4, 2026).
[104] *See generally* GAO-25-107088, *supra* note 26; *The Life Cycle of Scams*, BLOCK, Jan. 31, 2025, https://block.xyz/inside/the-life-cycle-of-scams.
[105] *See generally* GAO-25-107088, *supra* note 26.
[106] *Id.* at 8.
[107] FTC Fraud Reports Data, *supra* note 11.
[108] *Id.*
[109] GAO-25-107088, *supra* note 26, at 8.
[110] *AI Deepfake Concerns See Gen Z "Swiping Left" on Dating Apps*, BARCLAYS (Feb. 13, 2026), https://home.barclays/news/press-releases/20260/02/ai-deepfake-concerns-see-gen-z--swiping-left--on-dating-apps/.
[111] GAO-25-107088, *supra* note 26, at 9.
[112] *See generally id.*
[113] *Id.* at 9.

originated on social media,[114] with 72 percent of the fraud and scam attempts resulting in a reported dollar loss.[115] Overall, fraud and scam attempts initiated on social media accounted for over $2 billion in reported losses.[116] The typical lifecycle of a scam perpetrated on a dating application is as shown in Exhibit A:

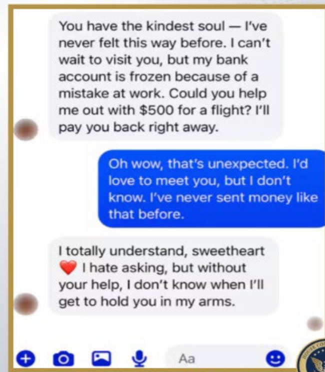
Exhibit A: Lifecycle of a Scam Initiated via a Dating Website[117]



[114] FTC Fraud Reports Data, *supra* note 11.
[115] *Id.*
[116] *Id.*
[117] Emma Fletcher, *Romance Scammers' Favorite Lies Exposed*, FED. TRADE COMM'N (Feb. 9, 2023), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed; *Account Picture: AI Dating Profile Picture Generator*, AIEASE, https://www.aiease.ai/ai-profile-picture-generator/dating/ (last visited June 4, 2026); *Personalization & Escalation Picture: 9 romance scams, and dating scammers' favorite lies*, NORTON, https://us.norton.com/blog/online-scams/romance-scams (last visited June 4, 2026); *Exit Image: Kim Pilling, Scrabble Romance Scam: Oldham woman, 83, Loses £20k to fraudster*, BBC (Feb. 14, 2024), https://www.bbc.com/news/uk-england-manchester-68298089; Patrick Allan, *How to Tell if a Tinder Profile is Fake*, LIFEHACKER (Apr. 26, 2016), https://lifehacker.com/how-to-tell-if-a-tinder-profile-is-fake-1772999305?test_uuid=zXnWOLjQQwkYjMVwrvo5w&test_variant=A.

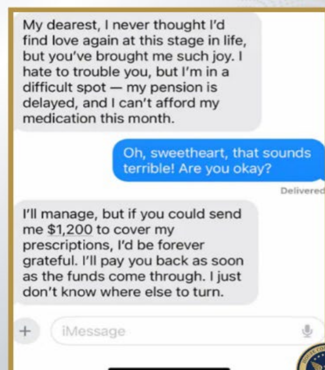
PERSONALIZATION

- Scammers then quickly work to build emotional intimacy with the intended victim.
- Often, fraudsters or scammers move communications to another platform to avoid monitoring.
- Scammers frequently leverage personal information from the intended victim's dating profiles and social media accounts to further build the relationship.



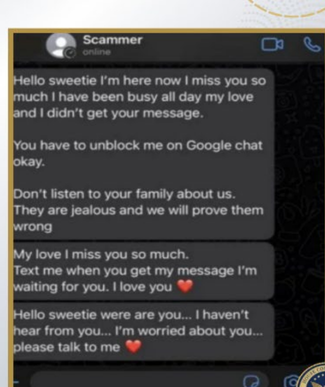
ESCALATION

- After building a personal relationship, scammers will claim that they have an emergency that requires immediate payment.
- Frequently, the claimed emergencies are medically related, or involve some form of imminent personal or legal risk.



EXIT

- Scammers may make additional requests for funds until the victim realizes they are being scammed. The scammers will then abscond with the victims' money.
- The most frequent method of payment requested is through gift cards.
- While making up a smaller number of transactions, bank transfers and digital assets represent the majority of reported financial losses.

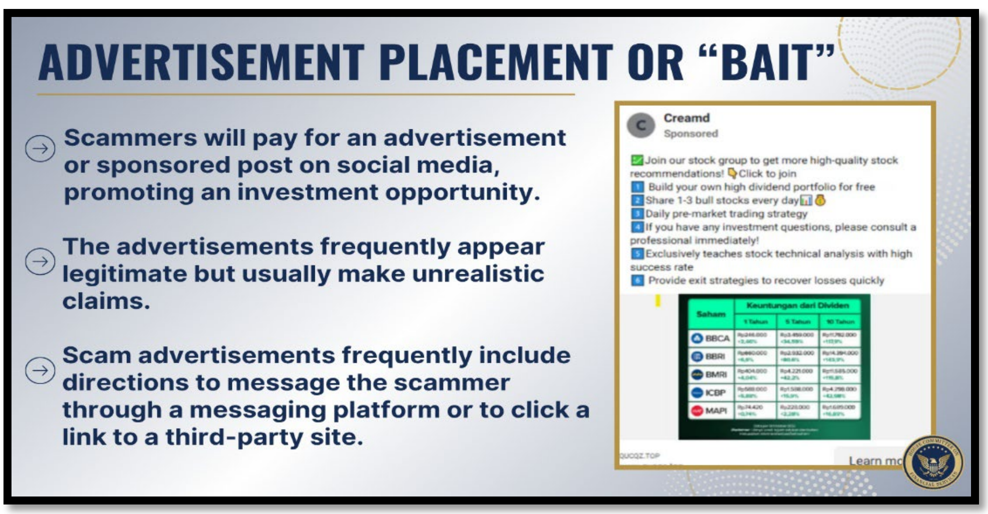


B. Fraud and Scams in Social Media Advertisements and Marketplaces

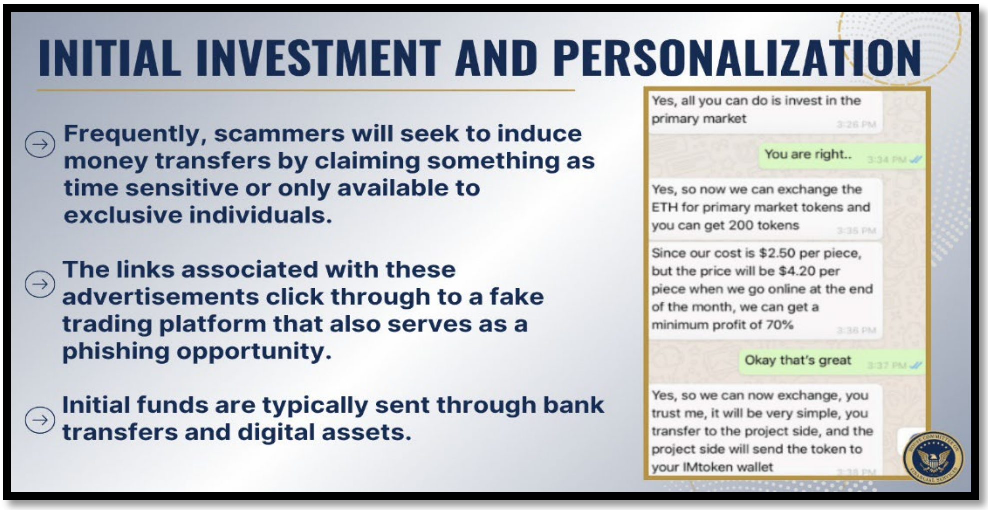
Social media marketplaces and advertisements are also being leveraged by fraudsters and scammers to make initial contact with their intended victims.[118] Often the schemes simply advertise a product that violates the marketplace policies, does not exist, or for which the scammer plans to ship an inferior product compared to what was advertised.[119] In other instances, advertisements and marketplace items are used to promote fake investments and jobs.[120] To facilitate these schemes, fraudsters and scammers will frequently purport to be a legitimate well-known retailer, subject matter expert, or government entity selling a product or providing an opportunity.[121]

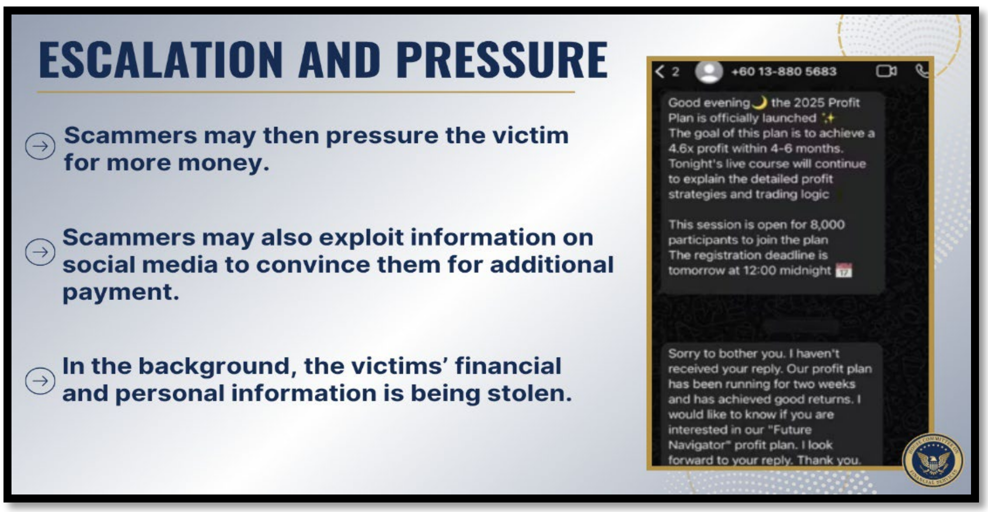
Given the enhanced scrutiny of advertisements and marketplace offerings compared to social media accounts, fraudsters and scammers have even greater incentives to extract large sums of money from victims.[122] The typical lifecycle of a scheme begun via false advertisements on social media is shown in Exhibit B.

Exhibit B: Lifecycle of a Scam Involving Spam Advertisements[123]

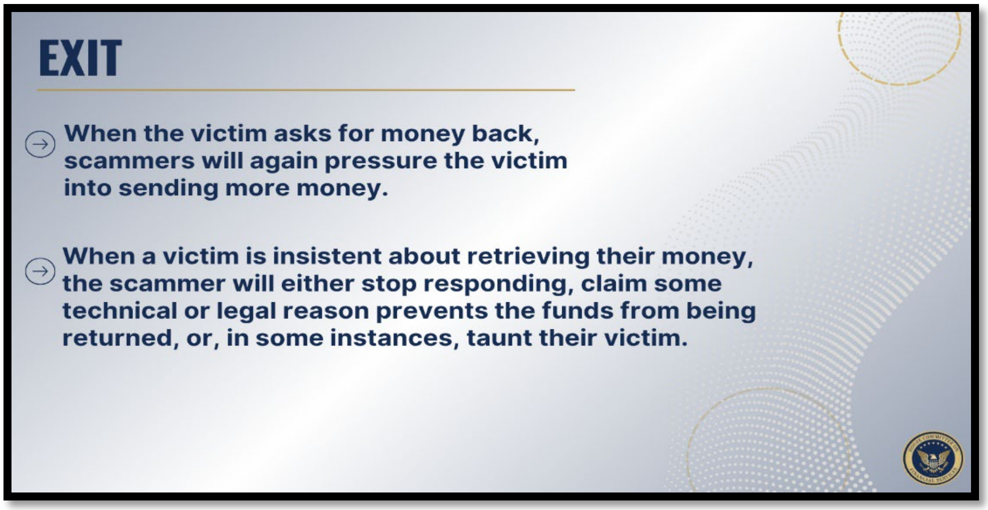


[118] Emma Fletcher, *Who's who in scams: a spring roundup*, FED. TRADE COMM'N (May 24, 2024), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/05/whos-who-scams-spring-roundup.
[119] *Don't Fall for These Online Marketplace Scams*, BANK OF HAWAII (Apr. 13, 2026), https://www.boh.com/blog/dont-fall-for-these-online-marketplace-scams.
[120] *Media Facts: Facts About Social Media Scams*, ZELLE, https://www.zelle.com/social-media-scams (last visited June 4, 2026)
[121] *Online and Digital Scams*, OFF. OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/online-and-digital-scams.html (last visited May 26, 2026); BANK OF HAWAII, *supra* note 119.
[122] SOCIAL MEDIA: CONTENT DISSEMINATION AND MODERATION PRACTICES, R46662, CONG. RESEARCH SERV. (2025).
[123] Li Han Tan, *The Dark Side of Social Media*, F-SECURE (Mar. 21, 2025), https://www.f-secure.com/en/partners/insights/the-dark-side-of-social-media-how-to-identify-investment-scams; *7 Ways To Spot Common Crypto Scams If You're Planning To Invest In*, SAYS (Feb. 17, 2023), https://says.com/my/tech/common-crypto-scams-to-look-out-for; *Top Scams of 2024*, FED. TRADE COMM'N (Mar. 10, 2025),





https://consumer.ftc.gov/consumer-alerts/2025/03/top-scams-2024; *Social Media and Stock Tip Scams,* U.S. SEC. & EXCH. COMM'N (Feb. 6, 2026), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins/social-media-stock-scams.



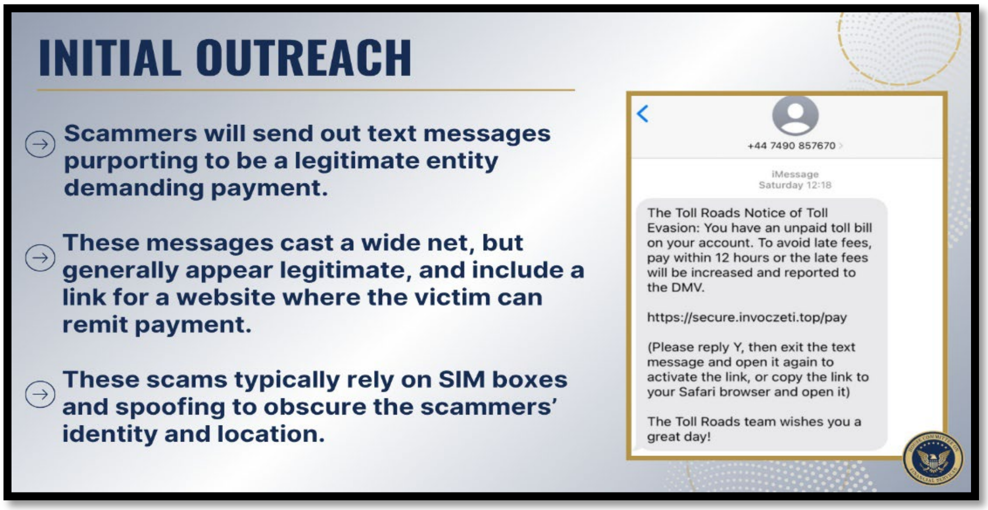
Social media advertisements and marketplaces have proven to be effective vectors of attack for fraudsters and scammers. Moreover, some platforms are more susceptible to fraud and scams depending on how much friction they implement into the process for their advertisers and users.[124] The unique, personal, and global nature of social media makes it a reliable tool for fraudsters and scammers to contact their victims and creates substantial challenges for social media companies and industries implicated throughout the fraud lifecycle in preventing or mitigating these schemes.

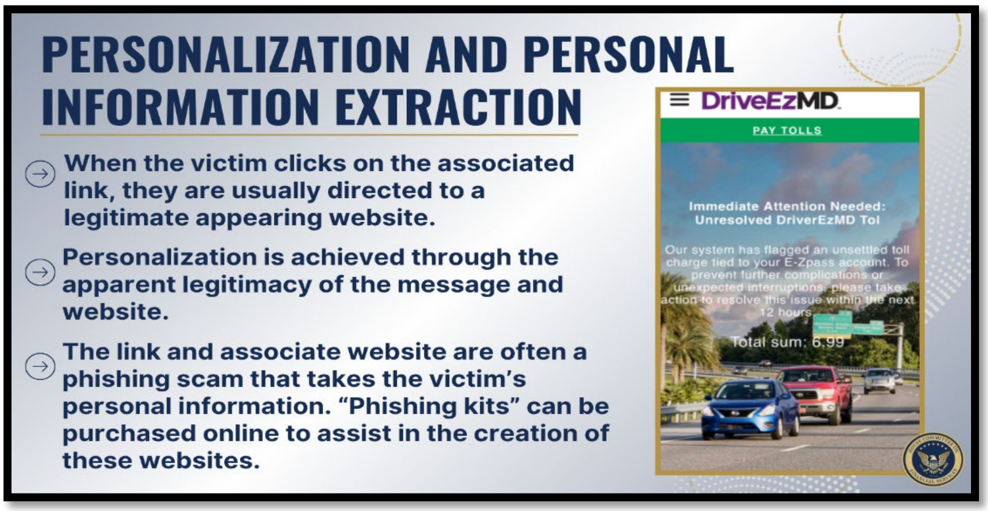
C. Text & Email-Enabled Fraud and Scams

Text messages and emails are a high-volume contact method for fraudsters and scammers that exploit several vulnerabilities across multiple industries. Typically, scammers will text from a spoofed phone number,[125] often presenting themselves as an authority figure, government agency, business, or financial institution.[126] The victim will be directed to click a link within the message, which takes them to a third-party website where the victim can submit their payment information.[127] The link within scam messages typically redirects the victim to a website that is also a phishing attempt of its own.[128] Additionally, scam messages often include a call to action directing the victim to remit payment by entering bank or credit card information on that third-party website.[129] The lifecycle of a scam originating via text message is as shown in Exhibit C.

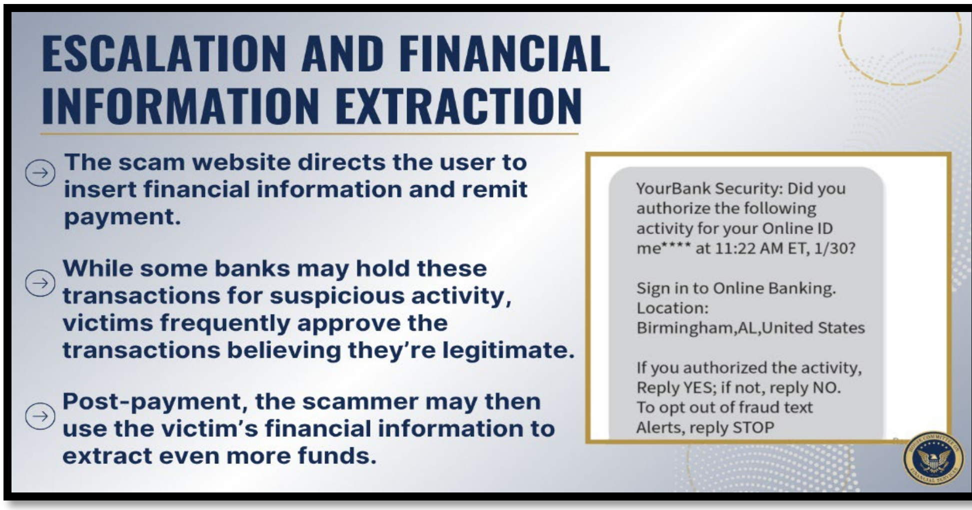
[124] *Limited ad serving*, GOOGLE, https://support.google.com/adspolicy/answer/13889491?hl=en (last visited June 4, 2026).
[125] *Unwanted Communications: Robocalls, Caller ID Spoofing, and Do-Not-Call Registry*, FED. COMMC'NS COMM'N, https://www.fcc.gov/enforcement/topics/unwanted-communications (last visited June 4, 2026); Press Release, Fed. Trade Comm'n, *supra* note 22.
[126] *Imposter Scams*, USAGOV, https://www.usa.gov/imposter-scams (last visited May 26, 2026).
[127] *Attorney General Schwalb Warns District Residents About Fake Toll Collection Scams*, DISTRICT OF COLUMBIA ATT'Y GEN. OFF. (May 13, 2025), https://oag.dc.gov/release/attorney-general-schwalb-warns-district-residents.
[128] *Smishing: Package Tracking Text Scams*, U.S. POSTAL INSPECTION SERV. (May 19, 2025), https://www.uspis.gov/news/scam-article/smishing-package-tracking-text-scams.
[129] *10 Text Message Scams You Didn't Know About (Until Now)*, FIRST BANK & TRUST CO. (July 1, 2024), https://www.firstbank.com/resources/learning-center/10-text-message-scams-you-didnt-know-about-until-now/.

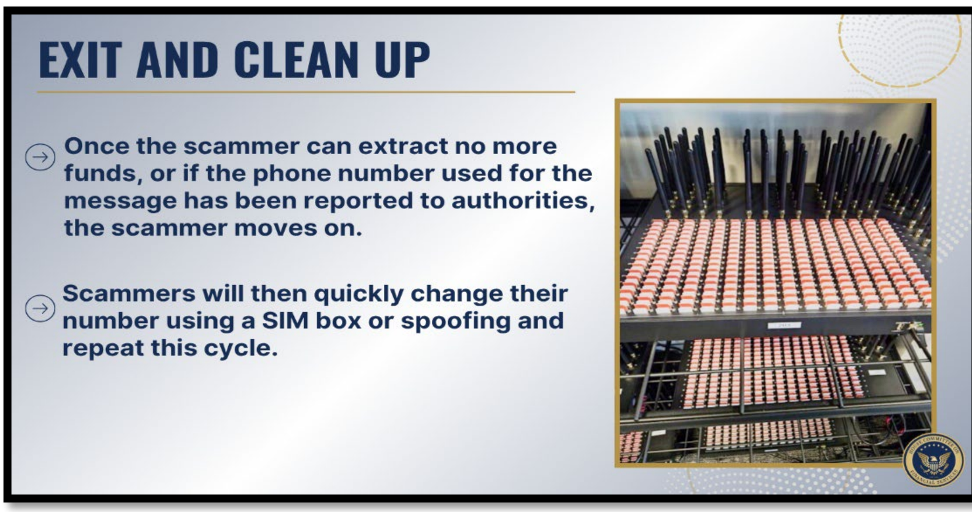
Exhibit C: Lifecycle of a Scam Involving Spam Texts[130]





[130] Tom Brennan, *Officials Warn of E-ZPass Text Scam*, WBJB (Feb. 18, 2025), https://www.wbjb.org/local-news/2025-02-18/officials-warn-of-e-zpass-text-scam; DISTRICT OF COLUMBIA ATT'Y GEN. OFF., *supra* note 127; Doug Segrest, 5 *Signs of a Scam Message*, REGIONS BANK (Feb. 1, 2022), https://doingmoretoday.com/5-signs-of-a-scam-message/; Shawn Chen & Julie Walker, *How a SIM Farm Like the One Found Near the UN Threatens Telecom Networks*, AP NEWS (Sep. 23, 2025), https://apnews.com/article/unga-sim-farm-threat-explainer-5274ccc927ab180a1d5e0ffd475ed7c9.





Combined, fraud and scam attempts initiated through text messages and emails accounted for over 770,000 reported fraud and scam attempts and just over $1.1 billion in losses.[131] In 2025, text messages replaced email as the most common point of initial contact for fraudsters and scammers, representing the initial point of contact for 23 percent of fraud and scam attempts.[132] While email was the most common means of initial contact in 2023 and 2024, representing approximately 25 percent of initial contact in those years,[133] its share reduced to 21 percent of initial outreach attempts for fraudsters and scammers in 2025.[134]

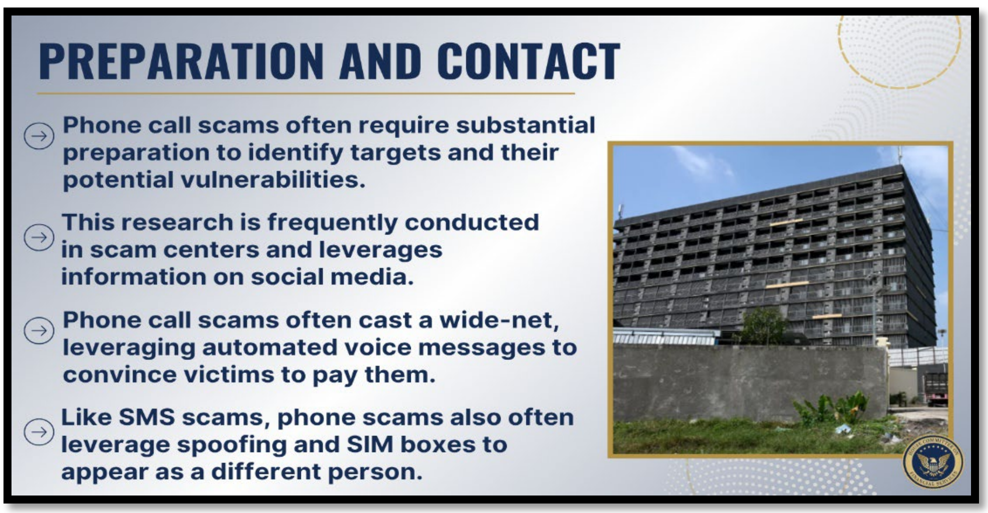
---

[131] FTC Fraud Reports Data, *supra* note 11.
[132] *Id.*
[133] *Id.*
[134] *Id.*

D. Fraud and Scam Outreach through Phone Calls

Fraud and scams perpetrated through phone calls can be as simple as an automated call or voicemail message that is sent out to a large number of people.[135] Conversely, the most alarming fraud and scam efforts initiated through phone calls often require the scammer to conduct a substantial amount of research on their intended victim.[136] This research can include identifying family members, finding out what bank the victim uses, and tailoring their scheme to the victim's geographic area, educational background, or other information that can be leveraged to build credibility and exploit the victim's emotions.[137] Fraudsters and scammers can also leverage AI to increase their call volume, clone the voices of specific individuals, or mask the natural voice of the fraudster or scammer making the call.[138] Phone calls are a particularly effective contact method for lower volume, higher value imposter scams. The typical scam taking place over the phone generally follows the path depicted in Exhibit D.

Exhibit D: Lifecycle of a Scam Originating via Phone Call[139]



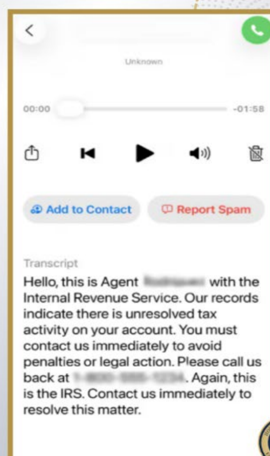
[135] GAO-25-107088, *supra* note 26, at 8-9.
[136] Biprojit Chakraborty, *What is Vishing? Voice Phishing Explained with Examples & Prevention Tips*, CloudEagle.ai, Sept. 26, 2025, https://www.cloudeagle.ai/blogs/what-is-vishing.
[137] *See* Kendra Cherry, *There's a Reason Even the Smartest People Fall for Scams*, VeryWellMind (Mar. 23, 2026), https://www.verywellmind.com/why-we-fall-for-scams-8705528.
[138] Amy Bunn, *Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam*, McAfee (May 15, 2024), https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/.
[139] Michael Sullivan & Greg Dixon, *A Crackdown on the Online Scam Epicenter of the World*, NPR (Feb. 27, 2026), https://www.npr.org/2026/02/27/nx-s1-5729583/a-crackdown-on-the-online-scam-epicenter-of-the-world; Mark Birchall, *IRS Scam Calls: How to Tell if an IRS Call Is Fake*, Norton (Mar. 27, 2026), https://us.norton.com/blog/online-scams/fake-irs-calls.

CREDIBILITY BUILDING

- The scammer will often appear to be a relative or another individual, business, or entity that the victim trusts.
- Scammers will sometimes leverage AI to clone the voices of other people, including relatives.
- Frequently, the scammer will reference information relevant to the victim to build their credibility.
- Alternatively, scammers may imitate government or law enforcement agencies.

PRESSURE AND ESCALATION:

- In scams where the scammer is pretending to be a loved one, the scammer will typically claim to need funds urgently, often for a legal or medical expense.
- In scams where the scammer is purported to be a law enforcement officer, the scammer will often threaten the victim with administrative or legal action.



EXIT

- Once payment is made, the scammer will simply hang up.
- Scammers will then change their numbers using a SIM box or spoofing, aiming to avoid law enforcement attention.
- Changing phone numbers frequently also compromises the ability of law enforcement and telecommunications firms to flag the suspect phone number
- Changing numbers increases the likelihood that scammers can retarget the same victim.

Phone calls were also a common point of initial contact between fraudsters and scammers, accounting for 17 percent of initial contact attempts in 2025.[140] This accounted for over $1.1 billion in fraud and scam losses on their own.[141] As recently as 2021, phone calls were the initial point of contact for 35 percent of all fraud and scam attempts, driven primarily by robocalls.[142] Recent actions by the Federal Communications Commission (FCC), cell phone makers, and telecommunications firms have substantially reduced the prevalence of robocalls, which, coupled with increased consumer awareness, have reduced telecommunications representation in initial contact attempts.[143] But more work is needed in this area.

E. Internet-Enabled Fraud and Scams

Fraud and scam attempts initiated through fake websites and pop-up advertisements operate like text and email scams. These schemes typically involve directing a victim to click a link or go to a website that will skim their personal and financial information.[144] Frequently, these websites and pop-ups will purport to be payment platforms for goods and services, or for the payment of private or government debt.[145] Through the website and pop-ups, the fraudster or scammer will seek to induce payment by the victim.[146] These outreach methods are also associated with ransomware attacks and cyber-blackmail attempts.[147]

Despite being a common fraud and identity theft vector in the nascent stages of consumer computer and internet usage, fraud and scams initiated through fraudulent or scam websites and pop-up advertisements represented just 13 and 3 percent of reported fraud and scam attempts in 2025, respectively.[148] Scam websites accounted for the initial point of contact in $1.116 billion in reported fraud and scam losses, while losses through fraudulent or scam pop-up advertisements were $265 million.[149]

COMMON FRAUD SCHEMES & SCAMS

A. Common Types of Fraud Schemes

Financial fraud encompasses a wide range of schemes. Perpetrators are employing increasingly sophisticated methods to gain unauthorized access to financial accounts and

---

[140] FTC Fraud Reports Data, *supra* note 11.
[141] *Id.*
[142] *Id.*
[143] *See e.g.*, 47 C.F. R. § 64 (2025); *TRACED Act Implementation*, FED. COMMUNICATIONS COMM'N, May 1, 2023, https://www.fcc.gov/TRACEDAct.
[144] *Online and Digital Scams*, FED. TRADE COMM'N, https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/online-and-digital-scams.html (last visited June 4, 2026).
[145] *Id.*
[146] *Id.*
[147] *Ransomware*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware (last visited June 4, 2026).
[148] FTC Fraud Reports Data, *supra* note 11.
[149] *Id.*

payment systems.[150] The following categories represent some of the most prevalent types of financial fraud affecting U.S. consumers and businesses today.

- *Credit Card and Debit Card Fraud.* Credit and debit card fraud involves the unauthorized use of a consumer's payment card credentials to make purchases or withdraw funds.[151] Card-not-present fraud, which is used in e-commerce and telephone transactions where the physical card does not need to be presented, has become a dominant subcategory.[152] This enables criminals operating anywhere in the world to exploit stolen card data without ever possessing the physical card.[153] Card credentials are typically obtained through data breaches, phishing attacks, card skimming devices, or purchases on criminal marketplaces.[154] The United States is disproportionately affected by card fraud relative to its share of global card transactions.[155]

- *Account Takeover Fraud.* Account takeover (ATO) fraud occurs when a criminal gains unauthorized access to a consumer's or business's financial account and initiates fraudulent transactions or drains account funds.[156] Like credit card fraud, account information is typically stolen through phishing attacks, malware, or data breaches.[157] ATO attacks are increasingly automated, with criminals using AI-powered tools to test vast numbers of stolen username and password combinations across multiple platforms simultaneously.[158] Once inside an account, criminals may initiate wire transfers, change account credentials to lock out the consumer, or use the account as a staging point for additional fraud.[159]

---

[150] Press Release, Fed. Bureau of Investigation, FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence (May 8, 2024), *available at* https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence.
[151] *Credit Card and Debit Card Fraud*, OFF. OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/credit-card-and-debit-card-fraud.html (last visited May 26, 2026).
[152] *What is card-not-present fraud? What businesses need to know*, STRIPE, https://stripe.com/resources/more/what-is-card-not-present-fraud-what-businesses-need-to-know (last visited May 26, 2026).
[153] *Id.*
[154] *Id.*; Kathryn Kandra, *The Dark Web Has You! (And Your Credit Card Information)*, ELLIPSE, https://www.ellipse.la/post/the-dark-web-has-you-and-your-credit-card-information (last visited May 26, 2026).
[155] The Nilson Report, *Global Card Fraud Losses at $33 Billion*, YAHOO!FINANCE (Jan. 7, 2026), https://finance.yahoo.com/news/global-card-fraud-losses-33-170800960.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMdBqHxXD2uhdxvmQH9CtbjnZNZRa43NmD4hmvzxRqCeJafy60p2TEYZH5gViUo8yXrC9bO8wsJUQEs2BX4EThGeZc75YUL5ASXTj8-Eh1U4obZ-7769Y_twpt99lCOPU1JjAFH2GZ90ocsKGarQAyytYuK-Q_ZkG95wNOPPTvZe.
[156] *Account takeover Fraud (ATO)*, INTERNET CRIME COMPLAINT CTR., https://www.ic3.gov/CrimeInfo/AccountTakeover (last visited May 26, 2026).
[157] *Id.*
[158] Emily Otto, *Beware of AI-enhanced Cyberattacks*, CEPA (Jan. 30, 2024), https://cepa.org/article/beware-of-ai-enhanced-cyberattacks/.
[159] *FBI Warns of Surge in Account Takeover Scams Targeting Everyone*, DIAMOND CREDIT UNION, https://diamondcu.org/blog/takeover-scams/ (last visited May 26, 2026).

- *Check Fraud.* Check fraud encompasses a range of schemes involving theft, forgery, or alteration of paper checks.[160] The most prevalent scheme currently is check washing.[161] This process involves criminals stealing checks from the mail, chemically removing the original payee and dollar amount, and rewriting the check to a new payee for a larger sum.[162] Occasionally, stolen checks and washed checks are available for purchase on criminal marketplaces.[163] The surge in mail theft over recent years has provided criminals with an abundant supply of checks. Despite the overall decline in check usage, check fraud has grown substantially as the relative ease of the scheme and lag time before detection make it an attractive scheme for criminals.[164]

- *Business Email Compromise.* Business email compromise (BEC) involves criminals sending emails that appear to originate from a trusted source, such as a Chief Executive Officer, vendor, or an attorney.[165] These emails may direct an employee to initiate a payment to a fraudulent account.[166] BEC schemes exploit the apparent trustworthiness of the sender and often target accounts payable staff, financial collectors, or executives with payment authority.[167] Criminals may compromise an actual email account through phishing or may spoof a legitimate address with subtle variations designed to evade detection.[168]

- *Synthetic Identify Fraud.* Synthetic identity fraud involves criminals fabricating new identities by combining real Social Security numbers with fictitious names, dates of birth, and addresses.[169] These fabricated identities are cultivated over time: criminals open accounts, make small purchases, and build credit before ultimately maxing out credit lines before disappearing.[170] Synthetic identity fraud is particularly difficult to detect because the fabricated data used by criminals is often a mix of real and fake

---

160 FIN. CRIMES ENF'T NETWORK, FINANCIAL TREND ANALYSIS, MAIL THEFT-RELATED CHECK FRAUD: THREAT PATTERN & TREND INFORMATION, FEBRUARY TO AUGUST 2023 (2024), *available at* https://www.fincen.gov/system/files/shared/FTA-Check-Fraud-FINAL508.pdf.
161 *Check Fraud Schemes*, FIRST CMTY BANKERS, https://www.firstcommunitysc.com/about/fraud-education/check-fraud-schemes (last visited May 26, 2026).
162 FIN. CRIMES ENF'T NETWORK, *supra* note 160.
163 *Id.*
164 Ted Simons, *Check theft and fraud are on the rise: What financial institutions can do about it*, THOMSON REUTERS (Sep. 11, 2023), https://www.thomsonreuters.com/en-us/posts/government/check-fraud/.
165 *Business Email Compromise*, FED. BUREAU OF INVESTIGATIONS, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise (last visited May 26, 2026); *What is business email compromise (BEC)?*, MICROSOFT, https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec (last visited May 26, 2026).
166 *Business Email Compromise (BEC)*, AMERICANBANK, https://www.ambk.com/security/business-email-compromise-bec/ (last visited May 26, 2026).
167 MICROSOFT, *supra* note 165.
168 Leslie Reardon, *Protecting Your Business from Business Email Compromise*, MONEY MATTERS (Jan. 20, 2026), https://moneymatters.busey.com/busey-bank-protecting-your-business-from-business-email-compromise-1.
169 Tom Sullivan, *Synthetic identity fraud: How to detect and prevent it*, PLAID (Jan. 15, 2026), https://plaid.com/resources/fraud/synthetic-identity-fraud/.
170 *Id.*; *How to Prevent Bust-Out Fraud and Synthetic Identity Risk*, TRANSUNION (Feb. 3, 2025), https://www.transunion.com/blog/how-to-prevent-bust-out-fraud.

data.[171] Further, the fabricated identity may pass automated verification checks that would flag inconsistencies in a real person's credit profile.[172]

B. Common Types of Payment Scams

As discussed, payment scams generally fall outside of the statutory liability framework for financial institutions, meaning consumers typically bear financial responsibility. Like fraud, scams are evolving rapidly due to AI, deepfakes, and other advanced technologies.[173] The combination of these developments makes scams harder to detect and more costly for victims.[174] The following categories are among the most common and impactful scams affecting American consumers and businesses today.

- *Imposter Scams.* Imposter scams involve criminals posing as trusted individuals or institutions like government agencies (*e.g.*, Internal Revenue Service, Social Security Administration, or law enforcement), financial institutions, technology companies, employers, or family members.[175] These scams pressure victims into sending money or sharing personal information.[176] Criminals frequently layer these schemes to create the appearance of legitimacy. A victim may first be contacted by a fake bank fraud specialist and is then transferred to a fake federal agent who instructs them to move funds to a secure account to protect the victim from an alleged ongoing crime.[177] Sub-categories exist as well, including government impersonation, business impersonation, tech support, or family emergency scams.[178]

- *Romance Scams.* Romance scams involve criminals cultivating fake romantic or personal relationships with victims over extended periods.[179] As noted above, criminals often initiate these scams through dating apps, social media, or messaging platforms before exploiting the emotional connection to solicit money or investments.[180] This period, which may last weeks or months, distinguishes romance

---

[171] Sullivan, *supra* note 169.
[172] *Id.*
[173] U.S. DEP'T OF HOMELAND SEC., IMPACT OF ARTIFICIAL INTELLIGENCE ON CRIMINAL AND ILLICIT ACTIVITIES (2024), *available at* https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf.
[174] Sari Harrar, *AI Makes It Next to Impossible to Detect Scams. Now What?*, AARP (Mar. 19, 2026), https://www.aarp.org/money/scams-fraud/detecting-ai-fraud/; Kevin Collier, *Scams could now cost Americans $119 billion a year, study finds*, NBC NEWS (Mar. 11, 2026), https://www.nbcnews.com/tech/security/scam-cost-price-money-crypto-what-to-do-help-rcna262722.
[175] USAGOV, *supra* note 126; Press Release, Fed. Bureau of Investigation, FBI Warns Public to Beware of Scammers Impersonating FBI Agents and Other Government Officials (June 5, 2024), https://www.fbi.gov/contact-us/field-offices/portland/news/fbi-warns-public-to-beware-of-scammers-impersonating-fbi-agents-and-other-government-officials.
[176] USAGOV, *supra* note 126.
[177] Alvaro Puig, *Did someone tell you to move or transfer your money? It could be a scam*, FED. TRADE COMM'N (Jan. 19, 2024), https://consumer.ftc.gov/consumer-alerts/2024/01/did-someone-tell-you-move-or-transfer-your-money-it-could-be-scam.
[178] USAGOV, *supra* note 126.
[179] *Stay Safe Online: Avoid Romance Scams*, U.S. SECRET SERV., https://www.secretservice.gov/investigations/romancescams (last visited May 26, 2026).
[180] *Id.*

scams from other imposter schemes and often results in victims transferring very large sums before detecting the deception.[181] Criminals may invest significant time and resources in building trust, frequently using fabricated backstories, stolen photographs, and scripted conversations to sustain the illusion.[182] Romance scam victims span all demographics, and the emotional manipulation involved makes victims less likely to report the crime due to shame or continued belief in the relationship.[183]

- *Investment Scams.* Investment scams involve criminals promising extraordinary returns from investment opportunities to induce victims into transferring funds to fraudulent platforms or accounts.[184] A particularly prevalent subcategory commonly known as "pig butchering" combines elements from romance, investment, phishing, and imposter scams into a scripted, long term, predatory scheme.[185] Criminals cultivate trust with victims, similar to a romance scam, and then gradually introduce fraudulent investment platforms that display fabricated profits to encourage larger deposits.[186] When victims attempt to withdraw their funds, they are assessed fake taxes or fees; ultimately, the scammer disappears with all deposited funds.[187]

- *Online Marketplace Scams.* Online marketplace scams involve fraudulent sellers on legitimate platforms advertising non-existent or misrepresented goods and collecting payment before disappearing.[188] Conversely, fake buyer scams target legitimate sellers by having the scammer make a fraudulent payment.[189] This allows criminals to collect shipped goods before the fraud is detected.[190] These scams exploit the trust consumers place in established marketplace platforms and the difficulty of verifying the identity and legitimacy of counterparties in digital transactions. The growth of peer-to-peer marketplace commerce has expanded the pool of potential victims and the volume of transactions available to exploit.[191]

---

[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] FBI 2025 INTERNET CRIME REPORT, *supra* note 25.
[185] *Investment Fraud and Pig Butchering*, U.S. SECRET SERV., https://www.secretservice.gov/investigations/investmentfraud-pigbutchering (last visited May 26, 2026).
[186] *Id.*
[187] *Cryptocurrency Investment Fraud*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud (last visited May 26, 2026).
[188] *Online and Digital Scams*, OFF. OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/online-and-digital-scams.html (last visited May 26, 2026).
[189] Alvaro Puig, *Selling stuff online? Here's how to avoid a scam*, FED. TRADE COMM'N (July 27, 2022), https://consumer.ftc.gov/consumer-alerts/2022/07/selling-stuff-online-heres-how-avoid-scam.
[190] *Id.*
[191] Jiayin Huang, *The Dark Side of Peer-to-Peer Marketplaces: Scams, Safety, and Regulation*, MEDIUM (Oct. 7, 2024), https://medium.com/@jiayinhuang0509/the-dark-side-of-peer-to-peer-marketplaces-scams-safety-and-regulation-57437764c61c.

- *Employment and Job Scams.* Employment or job scams involve posting fraudulent employment listings or directly contacting consumers with fake job offers.[192] These offers are often for remote positions requiring less experience and unusually high compensation.[193] Perpetrators pose as legitimate employers and direct victims to submit personal and financial information for onboarding purposes.[194] Victims may also be asked to participate in task-based schemes that involve moving money through the victim's own bank account, a practice that can expose the victim to criminal liability as an unwitting money mule.[195]

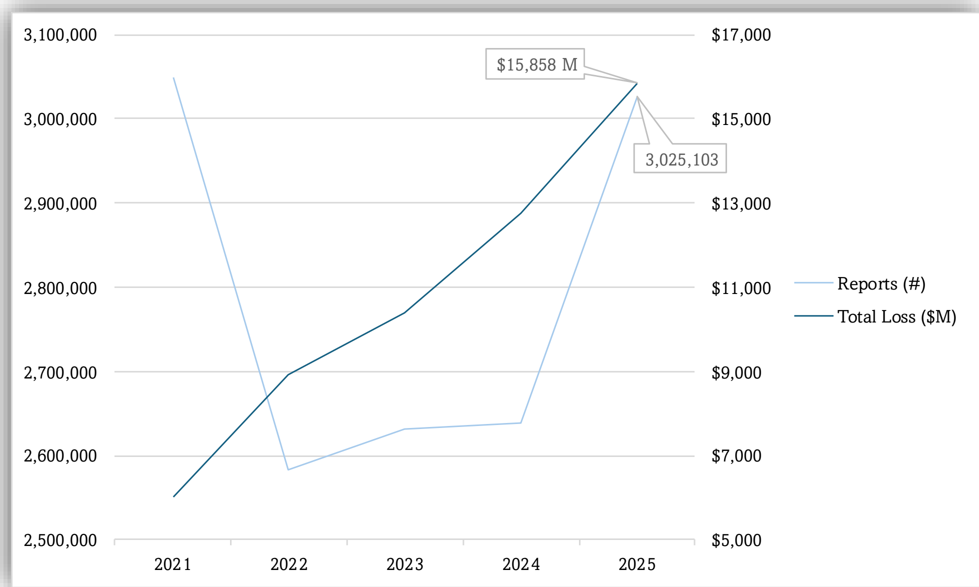
SCALE AND IMPACT OF FRAUD AND SCAMS

The prevalence of fraud and scams has continued to grow, reaching a high in 2025, with the FTC receiving over 3 million fraud reports from customers and a reported $15.9 billion in losses.[196] These losses represent a 27.5 percent increase compared to reported losses in 2024, which was also a record-breaking year at the time.[197] As compared to 2020, annual reported losses have increased approximately 430 percent.[198] Since the FTC began tracking fraud, scams, and identity theft statistics in 1997, the number of annual reports has increased by a staggering 1,800 percent.[199]

---

192 *Job Scams*, FED. TRADE COMM'N, https://consumer.ftc.gov/articles/job-scams (last visited May 26, 2026).
193 *Examples of Job Scams*, FED. TRADE COMM'N, https://consumer.ftc.gov/articles/job-scams#examples (last visited May 26, 2026).
194 Press Release, Fed. Bureau of Investigation, FBI Warns Cyber Criminals Are Using Fake Job Listings to Target Applicants' Personally Identifiable Information (Apr. 21, 2021), *available at* https://www.fbi.gov/contact-us/field-offices/elpaso/news/press-releases/fbi-warns-cyber-criminals-are-using-fake-job-listings-to-target-applicants-personally-identifiable-information.
195 *Id.*
196 *See J. Econ. Comm. Hearing*, *supra* note 11 (prepared testimony of Lois Greisman, Associate Director of the Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission).
197 *Id.*; *see also* Sarah Agostino, *Imposter Scams led Fraud Reports to the FTC for Fifth Straight Year in 2025, causing $3.5 Billion in Losses*, CNBC, June 26, 2026, https://www.cnbc.com/2026/06/26/imposter-scams-led-fraud-reports-to-ftc-in-2025-3point5-billion-losses.html.
198 *J. Econ. Comm. Hearing*, *supra* note 11 (prepared testimony of Lois Greisman, Associate Director of the Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission).
199 *Cf.* 2024 FTC DATA BOOK, *supra* note 12, at 6.

Exhibit E: Reports & Loss of Fraud and Scams 2021-2025[200]



Despite nearly $16 billion in reported losses to fraud and scams being staggering in its own right, the total value lost to these crimes is understood to be much higher. The FTC estimates that just two percent of fraud and scam attempts valued at under $1,000 and only seven percent of fraud and scam attempts valued over $1,000 are reported.[201] Using this data, the FTC estimates that Americans lost $195.5 billion to fraud and scams in 2024.[202]

What is clear from the data is that all Americans—regardless of background, age, or demographic—are vulnerable targets for fraud and scams. The Federal Reserve estimates that one in five Americans were the target or victim of financial fraud or a scam in 2024.[203] On average, the median reported loss ranged from approximately $300 to over $10,000, depending on the scheme.[204] Whereas certain segments of the population—such as the elderly—have historically been the primary target, the ever-evolving digital and technological landscape has expanded the pool of potential targets and increased the fraud and scam risk for all Americans.[205] Additionally, fraud and scams have an elevated rate of revictimization, meaning that once someone has become a victim of fraud or scams, they are more likely to become a victim again.[206]

---

[200] Derived from FTC Fraud Reports Data, *supra* note 11.
[201] FED. TRADE COMM'N, PROTECTING OLDER CONSUMERS 2024-2025 28 (2025).
[202] *Id.* Note, as of the time of publication, FTC had not published extrapolated numbers for 2025.
[203] BD. OF GOVS. OF THE FED. RSRV. SYS., ECONOMIC WELL-BEING OF U.S. HOUSEHOLDS IN 2024 3 (2025)
[204] FTC Fraud Reports Data, *supra* note 11.
[205] Emma Fletcher, *Not what you think: Millennials and fraud*, FED. TRADE COMM'N (Oct. 1, 2019), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2019/10/not-what-you-think-millennials-fraud.
[206] ASPEN INSTITUTE, A PERVASIVE THREAT, *supra* note 13.

A. A Closer Look at the Numbers

1. *Losses by Types of Fraud & Scams*

Investment scams amounted to $7.9 billion in losses reported to the FTC in 2025, representing half of all reported fraud losses.[207] In 2024, the median victim lost approximately $9,200 to investment-related scams, a figure 18 times higher than the median loss for all scams.[208] Further, investment scams also had the highest success rates among fraud and scams, with 79 percent of reported investments scams successfully taking money from consumers.[209]

Imposter scams amounted to $3.5 billion in losses reported to the FTC in 2025, making them the second largest category of reported losses.[210] In 2024, the median victim lost approximately $2,250 to business and job opportunity scams, a subset of imposter scams.[211] Romance scams, another subset, contributed nearly $1 billion in reported fraud losses.[212] Romance scams, like many other imposter scams, also have a long-term deleterious impact on victims that is impossible to quantify.[213] By manipulating their victims' trust to extract money, many of these scams create long-term mental health and relationship issues in their victims.[214] Combined, investment and imposter scams account for more than 70 percent of reported fraud losses.[215]

In terms of the number of reports, the FTC received over one million reports of attempted imposter scams in 2025, the most of any fraud or scam category.[216] Online shopping fraud and scam claims were the second most frequently reported, but the value lost in each of these scams is far lower than in other categories, amounting to $432 million in reported fraud losses for American consumers.[217]

---

[207] FTC Fraud Reports Data, *supra* note 11; *see also J. Econ. Comm.*, *supra* note 11 (prepared testimony of Lois Greisman, Associate Director of the Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission).
[208] FTC 2024 DATA BOOK, *supra* note 12, at 4.
[209] *Id.* at 8.
[210] FTC Fraud Reports Data, *supra* note 11.
[211] FTC 2024 DATA BOOK, *supra* note 12, at 4.
[212] FBI 2025 INTERNET CRIME REPORT, *supra* note 25, at 8.
[213] Balcombe, *supra* note 40.
[214] *Id.*
[215] FTC Fraud Reports Data, *supra* note 11.
[216] *Id.*
[217] *Id.*

Exhibit F: Top 10 Reported Fraud Categories in 2025[218]

Top 10 Fraud Categories

Rank	Category	# of Reports	% Reporting $ Loss	Total $ Loss	Median $ Loss
1	Imposter Scams	1,005,012	20%	$3,511.5M	$700
2	Online Shopping and Negative Reviews	419,098	78%	$446.4M	$117
3	Internet Services	193,911	19%	$209.3M	$300
4	Business and Job Opportunities	157,841	32%	$906.8M	$2,008
5	Investment Related	143,918	78%	$7,932.9M	$10,400
6	Telephone and Mobile Services	96,844	44%	$65.5M	$280
7	Health Care	82,868	55%	$77.7M	$275
8	Prizes, Sweepstakes and Lotteries	70,901	25%	$303.6M	$780
9	Travel, Vacations and Timeshare Plans	64,342	63%	$297.0M	$700
10	Advance Payments for Credit Services	51,327	37%	$100.8M	$768

The FBI also independently tracks reports of online crimes in its IC3 database. In 2025, the FBI received 452,868 fraud and scam complaints and identified $17.69 billion in online fraud and scam losses.[219] Similar to the FTC's findings, the FBI identified investment scams as the largest category of fraud losses, amounting to over $8.6 billion in 2025.[220] The reported losses to investment scams are not just the costliest category of fraud observed by the FBI, but they are the largest category of reported losses from any crime, of any type, committed online.[221]

[218] *Id.*
[219] FBI 2025 INTERNET CRIME REPORT, *supra* note 25, at 9.
[220] *Id.*
[221] *Id.* at 8.

Exhibit G: 2025 Crime Types & Associated Losses[222]

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

Although investment and imposter scams made up most fraud reports and losses for consumers, fraudsters and scammers target American consumers using a variety of other methods, including check fraud. Despite check usage having declined over 82 percent since 2000 due to the proliferation of credit and debit cards, wire services, payment applications, and digital assets, check fraud has remained commonplace.[223] Neither the FTC's nor the FBI's data aggregate the various types of check fraud into a single comprehensive estimate. However, at least one private sector estimate suggests that Americans lost as much as $24 billion to check fraud in 2024.[224]

---

[222] *Id.*
[223] Michael Cummins, *Checkmate on Checks Part One: The Decline of Paper Checks*, CITIZENS BANK, https://www.citizensbank.com/corporate-finance/insights/end-of-paper-checks.aspx (last visited May 26, 2026).
[224] REFINE INDUSTRIES, THE CHECK FRAUD KILL CHAIN: MOVING FROM DETECTION TO PREVENTION 2 (Sep. 9, 2024) (report prepared on behalf of the American Bankers Association), *available at* https://www.aba.com/news-research/analysis-guides/the-check-fraud-kill-chain.

2. *Victimization by Age Group*

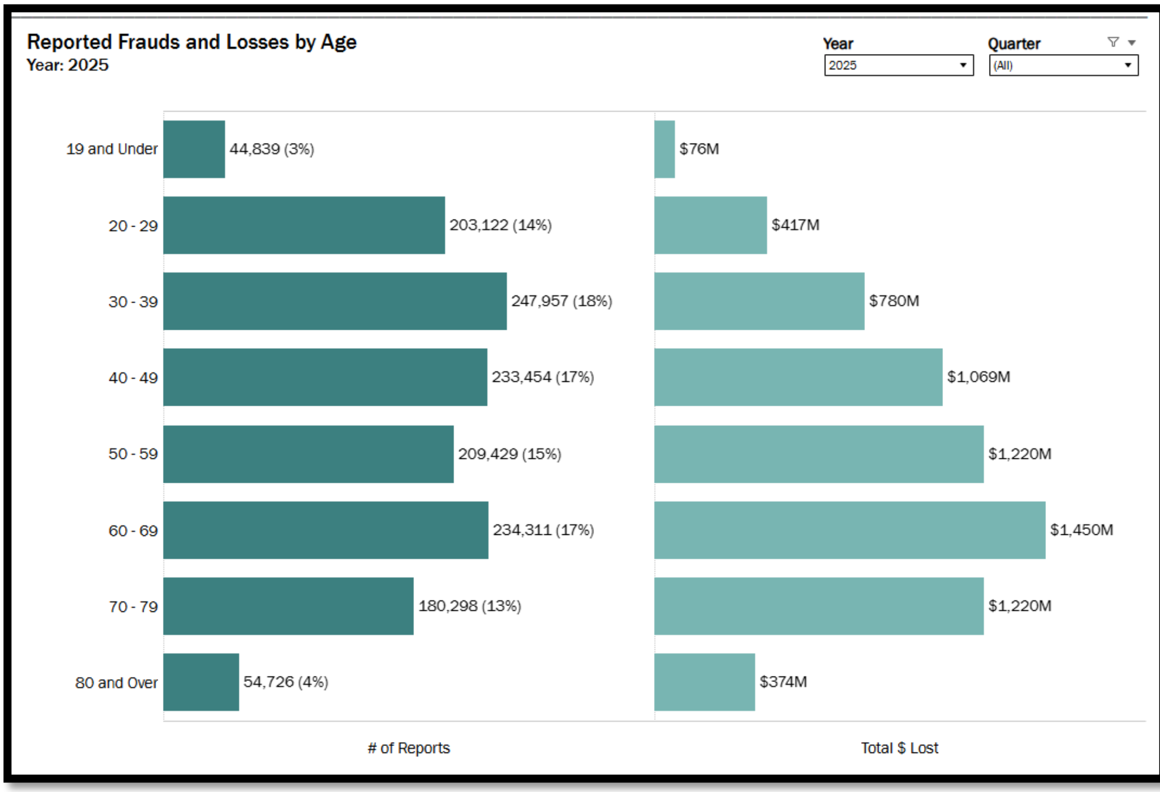
Overall, 38 percent of American adults report having been a victim of financial fraud and scams by age 50.[225] This percentage rises to 41 percent among American seniors.[226] Adults and seniors are generally preferred targets for scammers due to their higher average wealth, making individual fraud and scam attempts more profitable.[227] Compounding matters, scammers often target these individuals' retirement funds, which can be particularly devastating for seniors who have a more limited capacity to make money to offset their losses and often live on fixed incomes.[228]

Elderly Americans make such desirable scam victims that scammers design dedicated schemes, known as "grandparent schemes," to attack them.[229] In 2024, over thirty individuals in the United States and Canada were arrested in connection with a grandparent scam that stole over $21 million from American seniors.[230] In this scheme, the perpetrators would call elderly Americans from U.S.- or Canadian-based call centers and purport to be their relative in need of money.[231]

---

[225] Jessica McMaster, *4 in 10 Older Americans Have Lost Money to Fraud AARP Survey Finds,* AARP (Apr. 7, 2026), https://www.aarp.org/money/scams-fraud/fraud-awareness-survey-2026/?msockid=0adcb1146c5261c32bfda73d6dff607e.
[226] *Id.*
[227] *Scammers Target Older Adult Victims*, FED. BUREAU OF INVESTIGATION (May 15, 2026), https://www.fbi.gov/news/stories/scammers-target-older-adult-victims.
[228] ASPEN INSTITUTE, A PERVASIVE THREAT, *supra* note 13, at 3.
[229] Press Release, U.S. Immigration & Customs Enf't, 25 Canadian Nationals Connected to Nationwide Multi-Million Dollar "grandparent Scam" Charged in Vermont (Mar. 5, 2025) https://www.ice.gov/news/releases/25-canadian-nationals-connected-nationwide-multi-million-dollar-grandparent-scam.
[230] *Id.*
[231] *Id.*

Exhibit H: Reported Frauds & Losses by Age in 2025[232]



Young Americans have historically been seen as insulated from many fraud and scam risks.[233] On average, younger Americans have less wealth, making them a less desirable target.[234] Yet, modern trends suggest that fraud and scam risk is no longer correlated with the victim's age, as individuals under the age of thirty report more losses year-over-year.[235] Notably, while young people's familiarity with evolving technologies should provide them with a better understanding of suspect practices, particularly online, the success rate of fraud and scam attempts on Americans ages 20 to 29 is nearly twice the success rate for fraud attempts for seniors.[236] Further, recent data indicates that young Americans are increasingly at risk of online shopping scams and imposter scams.[237]

3. *Victimization by Educational Level*

The education level of fraud and scam targets has shifted substantially in recent years. In the past, the information and communications used to facilitate fraud and scam attempts accidentally included some type of formatting abnormality, typographical mistake, or some other

---

[232] FTC Fraud Reports Data, *supra* note 11.
[233] *Who Experiences Scams? A story for All Ages*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages (last visited May 26, 2026).
[234] *Scammers Target Older Adult Victims*, FED. BUR. OF INVESTIGATION (May 15, 2026), https://www.fbi.gov/news/stories/scammers-target-older-adult-victims.
[235] 2024 FTC DATA BOOK 2024, *supra* note 25.
[236] *Id.*
[237] FTC Fraud Reports Data, *supra* note 11.

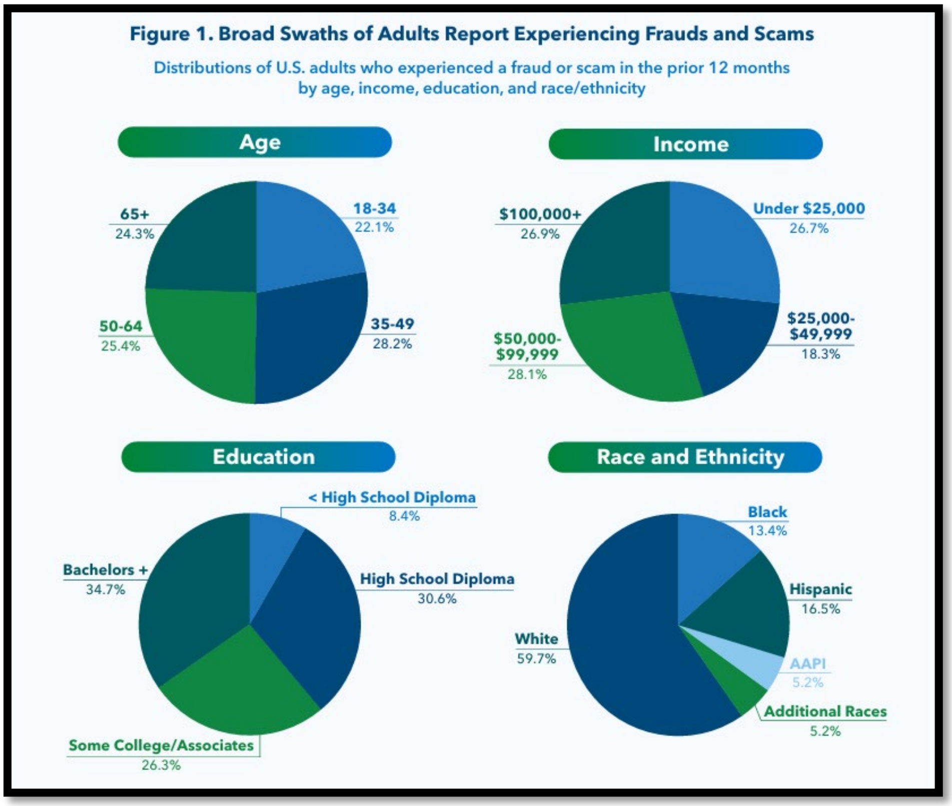
indicator that the referenced material or document may not be legitimate.[238] The criminals behind these schemes are aware that such mistakes are possible and have therefore sought out Americans they believed were less likely to notice such mistakes.[239] In fact, a substantial amount of the anti-fraud education material created by government agencies, companies, and academic institutions specifically advised Americans to look for such errors.[240]

With the rise of technologies like AI, fraudsters and scammers now have the tools necessary to create advertisements, communications, and other documents that are free of errors and appear legitimate enough to deceive even the most educated Americans.[241] For reference, in 2025, 36.9 percent of fraud reports were submitted by Americans with a bachelor's degree or higher,[242] which is roughly equivalent to their proportion of the population and reflects the growing equalization of risk across education levels.[243]

---

[238] NATIONAL CONSUMER LEAGUE, DEEPFAKES, CHATBOTS, AND SCAMS: HOW AI IS FUELING FRAUD AND WHAT POLICYMAKERS MUST DO 2 (2025).
[239] *Imposter Scams*, OFF. OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/imposter-scams.html (last visited May 26, 2026); *see also* MICROSOFT RESEARCH, WHY DO NIGERIAN SCAMMERS SAY THEY ARE FROM NIGERIA 11-12 (2012).
[240] *Recognize and Report Phishing*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/secure-our-world/recognize-and-report-phishing (last visited May 26, 2026).
[241] NATIONAL CONSUMER LEAGUE, *supra* note 238.
[242] ASPEN INSTITUTE, A PERVASIVE THREAT, *supra* note 13, at 5.
[243] U.S. Census Bureau, *supra* note 16.

Exhibit I: Demographic Breakdown of Adults Reporting Fraud & Scams[244]



4. *Victimization by Income*

Americans of all income levels are also similarly vulnerable to fraud and scams. High-income Americans are not at reduced risk due to having more resources, and Americans with lower incomes are also not insulated from fraud and scams despite having fewer resources to lose. Although Americans at all income levels are equally likely to be victimized by a fraud or scam, low-income Americans are much more likely to be revictimized.[245]

---

[244] ASPEN INSTITUTE, A PERVASIVE THREAT, *supra* note 13, at 4.
[245] *Id.* at 5.

Exhibit J: Reports of Fraud and Scams by Income Distribution[246]

	Number of Recent Frauds or Scams	
	One	Multiple
Age (mean)	51.3	50.6
Income Distribution		
Under $50,000	37.7%	44.7%
$50,000-$99,999	32.1%	27.6%
$100,000+	30.1%	27.7%

A notable example that exemplifies how neither income nor education can make you immune to fraud and scams occurred when Charlotte Cowles, a financial advice columnist for New York magazine, became the victim of a scam in 2024.[247] In this scheme, an individual pretended to be a CIA agent with detailed knowledge of Cowles's personal information and demanded that Cowles pay $50,000 to save Ms. Cowles and her family from imminent danger and to provide her with a new Social Security number.[248] Mr. Cowles put this money in a shoe box, taped it closed, and handed it to a courier.[249] This is just one example of a consumer being targeted despite her education.

5. *Victimization of Businesses*

In addition to individuals, businesses—particularly small businesses—are increasingly vulnerable to fraud and scams. Whereas individuals are protected from losses associated with unauthorized transactions (fraud), businesses tend not to have those same protections, meaning businesses must absorb the losses associated with both authorized and unauthorized fraudulent expenditures from their accounts.[250] According to one survey, of 200 business leaders in the United States, respondents reported losing an average of 9.8 percent of revenue to fraud and scams.[251] Notably, among just the 200 respondents, the reported losses amounted to $114 billion.[252] When extrapolated out to the vast number of U.S. companies, the amount lost to fraud and scams would likely reach into the trillions.

As with consumers, businesses of all sizes and across all industries are prone to fraud and scams. As an example, in 2024, Southern Oregon University (SOU) was the victim of a business

---

[246] *Id.*
[247] Ariel Zilber, *NY Magazine's Financial Advice Columnist Admits She Lost $50k to Scammer Claiming to be CIA Agent,* N.Y. POST (Feb. 15, 2024), https://nypost.com/2024/02/15/business/ny-magazines-financial-advice-columnist-lost-50k-to-scam/.
[248] *Id.*
[249] *Id.*
[250] 12 C.F.R. § 1005.2.
[251] *Fraud Costs Businesses Nearly 8 percent of Their Equivalent Revenues Globally*, *Transunion Reports*, TRANSUNION (Oct. 8, 2025), https://newsroom.transunion.com/h2-2025-global-fraud-report/.
[252] *Id.*

email compromise scheme.[253] In this scheme, fraudsters learned that SOU had recently agreed to terms with a contractor and presented themselves to SOU as the contractor in need of payment. After SOU remitted payment for these services, they were alerted that the real contractor had never received payment.[254] In total, SOU lost $1.9 million in this scheme that leveraged both business email compromise and social engineering.[255] The owner of a small landscaping business in Louisville, Kentucky also claimed to have lost money to scammers, who allegedly were able to access the business's payment accounts and transfer money used to pay employees.[256]

B. A Look at the Criminal Actors

A major shift in the landscape of fraud and scams is the background of the most prolific fraudsters and scammers. Historically, most scammers—particularly online scammers—were domestic actors working from their homes.[257] While this continues to be a common source of fraud and scam attempts, recently, transnational criminal organizations (TCOs) have taken on a major role in perpetuating these schemes and are increasingly responsible for losses from fraud and scams.[258] In fact, many criminal organizations engaged in the drug trade, smuggling, human trafficking, arms dealing, and other serious criminal activity have diversified their operations to include fraud and scams given its profitability.[259]

1. *Southeast Asian Scam Centers*

The most notable change in the profile of the perpetrators of fraud and scams has been the growth of large scam compounds (or "scam centers"), many of which are located in Southeast Asia, particularly Burma, Laos, and Cambodia.[260] One Administration official estimated there are as many as 150 scam centers in Southeast Asia which exist to scam foreigners.[261] These scam centers are generally overseen by Chinese criminal syndicates and rely heavily on human-trafficked laborers from China and other parts of Southeast Asia.[262] As many as 300,000 people have reportedly been trafficked to these compounds and subjected to forced labor and horrendous labor conditions.[263] In fact, at least one stakeholder stated that, "from a

---

[253] *University Loses $1.9 Million After Falling Victim to Business Email Compromise*, UNIV. OF CA RIVERSIDE (Apr. 24, 2024), https://its.ucr.edu/attack-alerts/2024/04/24/university-loses-19-million-after-falling-victim-business-email-compromise.
[254] *Id.*
[255] *Id.*
[256] Valerie Chinn, *Louisville Business Owner Says Scammers Drained his Account, Leaving Just 44 Cents*, WDRB (Apr. 7, 2026), https://www.wdrb.com/wdrb-investigates/louisville-business-owner-says-scammers-drained-his-account-leaving-just-44-cents/article_eaedf362-2f23-4c25-960f-d44ed7ece5ae.html.
[257] Jonathan Lusthaus, *The Cybercrime Industry*, 16 HARVARD NAT'L SEC. J. 195 (2025), *available at* https://journals.law.harvard.edu/nsj/wp-content/uploads/sites/82/2025/11/Lusthaus_16-Harvard-Natl-Security-J.-2-2025.pdf; Laila Bera, *Elevating Fraud and Scams as a National Security Threat*, ASPEN INST. (Nov. 27, 2025), https://fraudtaskforce.aspeninstitute.org/scams-as-national-security-threat.
[258] Bera, *supra* note 257.
[259] *Id.*
[260] *Id.*
[261] Briefing with House of Representatives staff (notes on file with the Committee).
[262] U.S.-CHINA ECON. & SEC. REVIEW COMM'N, CHINA'S EXPLOITATION OF SCAM CENTERS, *supra* note 18.
[263] U.N. HUMAN RIGHTS COMM'N, *supra* note 17.

payments perspective," Chinese organized crime are among the most concerning actors behind fraud and scams.[264]

Many scam centers operate in Special Economic Zones (SEZ) that were created under the People's Republic of China's (PRC) Belt and Road Initiative and are therefore subject to minimal oversight by their host nations.[265] Given that these scam centers are clustered in cities and localities that have been specifically designated as SEZs at the behest of the PRC government,[266] coupled with the reality that Chinese syndicates are overseeing these compounds,[267] it is highly unlikely that the PRC is not aware of these scam centers and their schemes.[268] Despite a lack of evidence of the PRC's direct involvement, national security officials believe the PRC is likely aware of and benefiting from these schemes.[269] Those officials argue that the PRC's interactions with TCOs are fostered "through the norms of selective enforcement and political protection that inherently shield criminal activity" with varying degrees of complicity.[270] In tolerating these organizations, the PRC alleviates pressure it faces from interstate criminal activity within its borders, while increasing its influence in foreign nations' financial ecosystems.[271] This is achieved by cracking down on Chinese scammer groups domestically, while allowing displaced networks to take root offshore.[272] These groups then entrench themselves within the weak structure of other countries' financial ecosystems, which ultimately leads to political influence over countries hosting these organizations.[273] Essentially, although not directly controlled, the PRC receives a real benefit internally and externally from these groups, which it can leverage to offset costs and bolster influence.[274]

Scam centers are prolific perpetrators of imposter and investment scams and are estimated to account for approximately $10 billion worth of fraud and scam losses in 2024.[275] They are also heavily associated with AI-enhanced romance scams. [276] As one Administration official described, these crime groups are perpetrating a "generational wealth transfer from Main Street America to the PRC and Southeast Asia."[277] In fact, scam centers have become so

---

[264] Briefings with Committee Republican staff (notes on file with the Committee).
[265] U.S.-CHINA ECON. & SEC. REVIEW COMM'N, CHINA'S EXPLOITATION OF SCAM CENTERS, *supra* note 18.
[266] *Id.*
[267] *Id.*
[268] *Id.*
[269] *Id.*
[270] SELECT COMM. ON THE STRATEGIC COMPETITION BETWEEN THE UNITED STATES & THE CHINESE COMMUNIST PARTY, CRIME, CORRUPTION, AND POWER: CCP-LINKED TRANSNATIONAL CRIME AND THE RISE OF A DISTRIBUTED THREAT TO U.S. NATIONAL SECURITY 8 (2026).
[271] *Id.* at 9.
[272] *Id.* at 25.
[273] *Id.* at 20.
[274] *Id.* at 19.
[275] Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams (Sep. 8, 2025), https://home.treasury.gov/news/press-releases/sb0237 [hereinafter Treasury Sanctions Southeast Asian Networks].
[276] News Release, Interpol, Interpol Releases New Information on Globalization of Scam Centers (June 30, 2025), https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres [hereinafter Interpol, Globalization of Scam Centers].
[277] Briefing with House of Representatives staff (notes on file with the Committee).

effective that they have begun franchising their model to other parts of the world, including the Middle East and Western Africa.[278]

2. *Latin American Cartels*

Other criminal organizations, such as Latin American drug cartels, have also begun participating in fraud and scam regimes.[279] They largely began participating during the COVID-19 pandemic as a means of compensating for their decreased income from illicit drug sales.[280] Fraud and scams now serve as an important hedge against similar, future uncertainty and provide cartels with more consistent cash flow and minimal upfront cost.[281] Further, with the rapid increase in the amount of funds being stolen by scammers, the scam industry now rivals the illicit drug trade in size and presents an opportunity for the cartels to make even more illicit money.[282] Law enforcement and experts have also found that cartels have received additional assistance refining their fraud and scam processes from increasingly close collaboration with Chinese networks across various other criminal enterprises.[283] Between 2021 and 2023, there was a 529 percent increase in the number of cyberattacks committed by Latin American cartels against Americans, many aimed at perpetrating a fraud or scam.[284] As the Director of Financial Services at the Consumer Federation of America, Mr. Adam Rust, testified, many of the organizations engaging in money laundering, the drug trade, and human trafficking have also started to engage in these scams because "it has become" a "new line of business" from which criminal organizations can make a profit.[285]

Interpol has indicated that specific cartels—such as Commando Vermelho, Primeiro Comando da Capital, and Cartel Jalisco New Generation (CJNG)—are involved in perpetrating financial fraud.[286] CJNG appears to possess particularly advanced fraud and scams infrastructure, having purportedly embraced AI and other tools to facilitate their schemes.[287] Further, CJNG has been particularly aggressive about recruiting operatives and victims through social media.[288] As Latin American cartels continue to build their relationships with other TCOs, such as Southeast Asian scammers and Chinese money laundering networks, they will likely delve further into the fraud and scam industry.

---

[278] Interpol, Globalization of Scam Centers, *supra* note 276.
[279] Bio, *supra* note 19.
[280] Alberto Aziani, et. al., *COVID-19 and Organized Crime: Strategies employed by criminal groups to increase their profits and power in the first months of the pandemic*, NAT'L LIBRARY OF MED. (Sep. 13, 2021), https://pmc.ncbi.nlm.nih.gov/articles/PMC8437330/.
[281] Bio, *supra* note 19.
[282] ASPEN INST., UNITED WE STAND: A NATIONAL STRATEGY TO PREVENT FRAUD AND SCAMS 8 (2025) [hereinafter ASPEN INST., UNITED WE STAND].
[283] U.N. OFF. ON DRUGS & CRIME, INFLECTION POINT: GLOBAL IMPLICATIONS OF SCAM CENTERS, UNDERGROUND BANKING, AND ILLICIT ONLINE MARKETPLACES IN SOUTHEAST ASIA 58 (2025).
[284] Bio, *supra* note 19.
[285] *Fighting Fraud on the Front Lines*, *supra* note 43 (statement of Mr. Adam Rust, Director of Financial Serv., Consumer Federation of America).
[286] *Interpol Financial Fraud Assessment: A Global Threat Boosted by Technology,* INTERPOL (Mar. 11, 2024), https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology.
[287] Bio, *supra* note 19.
[288] *Id.*

3. *Geopolitical Competitors*

U.S. geopolitical rivals and adversaries are also working to leverage these schemes to harm Americans and undermine U.S. interests.[289] Although proving that foreign non-state actors are functioning as an arm of their government is challenging, substantial evidence exists to suggest that, in addition to the PRC, the governments of Russia and North Korea are allowing or promoting these types of crimes against Americans.[290]

Russian scammer groups have been involved in a number of fraudulent schemes throughout the United States with links back to the Russian government.[291] In April 2022, the Treasury Department's Office of Foreign Asset Control (OFAC) sanctioned Garantex for its role in facilitating and supporting malicious cyber activities of darknet markets and ransomware groups within Russian borders.[292] Ransomware groups, in particular, are known to work as proxies for the Russian government and often avoid prosecution from the government due to their working relationship.[293] These groups have targeted critical cyber infrastructure throughout the United States and in the past several years have been tied to attacks on the Colonial Pipeline,[294] the DC Metropolitan Police Department,[295] and UnitedHealth Group.[296] Garantex played a role in laundering money for these groups, in addition to providing account and exchange services.[297]

In March 2025, a coordinated international law enforcement group made up of U.S. Secret Service, German, and Finnish authorities officially dismantled Garantex and arrested key administrators.[298] However, within days of the takedown, Garantex relaunched as Grinex and continued conducting business.[299] In August 2025, the Treasury Department executed a redesignation action, formally banning Grinex under cyber authorities.[300] In another instance of Russian-linked fraud activity in the United States, the Trump Administration announced in March 2026 that the Department of Justice (DOJ) had charged a Russian group with orchestrating a large-scale money laundering and Medicare fraud scheme.[301] The scheme

---

289 ASPEN INST., UNITED WE STAND, *supra* note 282.
290 *Id.*
291 Max Zuber, *Explaining Organizational Instability in Russian Ransomware Gangs*, Univ. of Wash. Jackson School of Int'l Studies (Oct. 16, 2023), https://jsis.washington.edu/news/explaining-organizational-instability-in-russian-ransomware-gangs/.
292 Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasions and Cyber Criminals (Aug. 14, 2025), https://home.treasury.gov/news/press-releases/sb0225 [hereinafter Treasury Sanctions Cryptocurrency Exchange].
293 Zuber, *supra* note 291.
294 *Id.*
295 Press Release, U.S. Dep't of Just., Ransomware Charges Unsealed Against Russian National (May 16, 2023), https://www.justice.gov/usao-dc/pr/ransomware-charges-unsealed-against-russian-national.
296 Geoff Brumfiel, *Pharmacies Struggle to Fill Prescriptions After UnitedHeath Ransomware Attack*, NPR, Mar. 1, 2024, https://www.npr.org/2024/03/01/1235255804/pharmacies-ransomware-prescriptions-unitedhealth.
297 Treasury Sanctions Cryptocurrency Exchange, *supra* note 292.
298 *Id.*
299 *Id.*
300 *Id.*
301 Press Release, U.S. Dep't of Just., Russian Citizen Charged with Laundering Over $1.2M Connected to $400M in Fraudulent Medicare Claims (Mar. 5, 2026), https://www.justice.gov/opa/pr/russian-citizen-charged-laundering-over-12m-connected-400m-fraudulent-medicare-claims.

entailed targeting Medicare Advantage Organizations (MAOs).[302] The group submitted over $400 million in false claims and obtained $1.7 million in reimbursement, which was then moved across multiple bank accounts.[303] Although the connection to the Russian state is unestablished, the ringleader, Nikolai Buzolin, and his co-conspirators, wired $1.2 million of the fraudulent proceeds back to Moscow.[304]

The North Korean government has also been implicated in fraud and scams targeting the United States.[305] In March 2026, OFAC sanctioned multiple individuals and two entities linked to the Democratic People's Republic of Korea's (DPRK) government-run information technology schemes, which are designed to generate illicit revenue for the regime's weapons-of-mass-destruction programs.[306] One of these information technology schemes, known as a "laptop farm" scheme, was uncovered by the DOJ in July 2024.[307] The plot entailed North Korean workers posing as U.S. citizens and obtaining remote information technology positions across 300 U.S. companies.[308] Once hired, the workers requested that the company mail the laptops to conspirators within the United States; the conspirators then modified the laptops so individuals could work from North Korea while appearing to work in the United States.[309] The scheme ended up accumulating more than $17 million in revenue for the North Korean government.[310]

Additionally, the DPRK has also used its infiltration of U.S. companies as a source of intelligence.[311] In certain instances, law enforcement found these North Korean workers introduced malware into company networks to extract proprietary and sensitive information from company systems.[312] The Treasury Department noted that, in the year 2024, it is estimated that these schemes generated approximately $800 million in revenue for the DPRK.[313] The DPRK has also had its hand in investment and romance scams throughout the United States.[314]

---

[302] *Id.*
[303] *Id.*
[304] *Id.*
[305] Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Facilitators of DPRK IT Worker Fraud Targeting U.S. Businesses (Mar. 12, 2026), https://home.treasury.gov/news/press-releases/sb0416 [hereinafter Treasury Sanctions Facilitators of DPRK IT Worker Fraud].
[306] *Id.*
[307] Press Release, U.S. Dep't of Just., Arizona Woman Sentenced in $17M IT Worker Fraud Scheme That Illegally Generated Revenue for North Korea (July 24, 2025), https://www.justice.gov/usao-dc/pr/arizona-woman-sentenced-17m-it-worker-fraud-scheme-illegally-generated-revenue-north.
[308] *Id.*
[309] *Id.*
[310] *Id.*
[311] Treasury Sanctions Facilitators of DPRK IT Worker Fraud, *supra* note 305.
[312] *Id.*
[313] *Id.*
[314] Press Release, Fin. Crimes Enft. 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.

C. A Look at the Tools & Tactics

1. *Artificial Intelligence*

AI is rapidly becoming one of the most powerful tools in the modern scammer's arsenal.[315] According to TRM Labs, "AI-enabled scam activity rose 500 percent over the last year,"[316] far outpacing the growth in traditional fraud. In a recent survey of over 5,000 U.S. adults, 12 percent reported being scammed with the use of AI,[317] a figure that is likely underinclusive given that AI can be difficult to identify. Projected losses from AI-enabled scams are expected to reach $40 billion by 2027.[318] The FBI took formal note of this alarming trend: for the first time in more than two decades, the agency tracked AI-related fraud in its annual cybercrime report, recording over 22,000 complaints tied to AI and totaling roughly $893 million in losses.[319]

The recent improvements in AI have enabled a new range of schemes and made certain older schemes more viable. Scammers can use generative AI, for example, to eliminate the telltale imperfections that once made scams detectable. It is possible for scammers and fraudsters to create highly realistic-looking emails and documents that lack the typos and formatting issues that were common in early phishing and imposter scams.[320] This creates perceived credibility in these documents or communications; resultingly, even the most savvy and diligent consumer may be unable to discern that the email or document they are reviewing is not legitimate.[321] AI can have a similar impact with romance scams, greatly increasing the quality and volume of fake photos, profiles, and accounts to lure in unsuspecting individuals.[322] And AI-generated phishing emails now achieve click-through rates more than four times higher than their human-crafted counterparts.[323] Voice cloning has also been one of the most rapidly weaponized capabilities: whereas scammers once mostly impersonated friends and relatives, by 2025 they went as far as impersonating U.S. officials, targeting current and former federal and state government officials

---

[315] NAT'L CONSUMER LEAGUE, *supra* note 29.
[316] *Modernizing the BSA for Financial Crimes in the 21st Century*, *supra* note 45 (statement of Ari Redbord, Global Head of Policy, TRM Labs).
[317] *See* UNITED STATES OF SCAMS, *supra* note 10, at 17.
[318] *AI Scams Explained: How AI-Powered Fraud Works and How Enterprises Detect It*, VECTRA, https://www.vectra.ai/topics/ai-scams.
[319] Maria Salette Ontiveros, *The FBI is Now Tracking AI Scams, and the Losses are Huge*, DALLAS MORNING NEWS (May 6, 2026), https://www.govtech.com/artificial-intelligence/the-fbi-is-now-tracking-ai-scams-and-the-losses-are-huge.
[320] News Release, Fed. Bureau of Investigation, FBI Warns of Increasing Threat of Cyber Criminals utilizing Artificial Intelligence (May 8, 2024), *available at* https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence.
[321] *Id.*
[322] U.S.-CHINA ECON. & SEC. REVIEW COMM'N, PROTECTING AMERICANS FROM CHINA-LINKED SCAM CENTERS: AN UPDATE ON EMERGING TRENDS 3-4 (2026) [hereinafter: U.S.-CHINA ECON. & SEC. REVIEW COMM'N, PROTECTING AMERICANS].
[323] *AI Scams Explained: How AI-Powered Fraud Works and How Enterprises Detect It*, VECTRA, https://www.vectra.ai/topics/ai-scams.

and their contacts.[324] In testimony before the Committee, National Director of the BankSafe Initiative at AARP, Ms. Jilenne Gunther, explained:

> Gone are the days where you can pinpoint a scam because someone is making a spelling error or a grammar mistake. They are using AI to write realistic messages. They are cloning people's voices. They are doing deepfake videos of people that they may know, so it makes those scams feel more credible. But also, [the use of technology] reduces the chance that consumers are really going to question that interaction. And that is why it is so important and critical to really look upstream with the first point of interaction between the criminal and the potential victim.[325]

Agentic AI can also be used by criminals to increase the speed and volume of scams. Through agentic AI, scammers can automate many aspects of the scam process, particularly in the context of romance scams, and allow them to convincingly reach more individuals more quickly.[326] This includes not only leveraging fake information and images created by generative AI, but also allowing communications with victims to be automated heavily, and to better compensate for language differences between the perpetrator and victim.[327]

The unfortunate reality is that around one in three instances of fraud involving AI is ultimately successful[328]—a sobering conversion rate that helps explain why criminal adoption of these tools has accelerated so dramatically. And in many cases, given developments in AI, victims face not only financial loss but an erosion of trust in digital communication and institutions.

2. *Payment Systems*

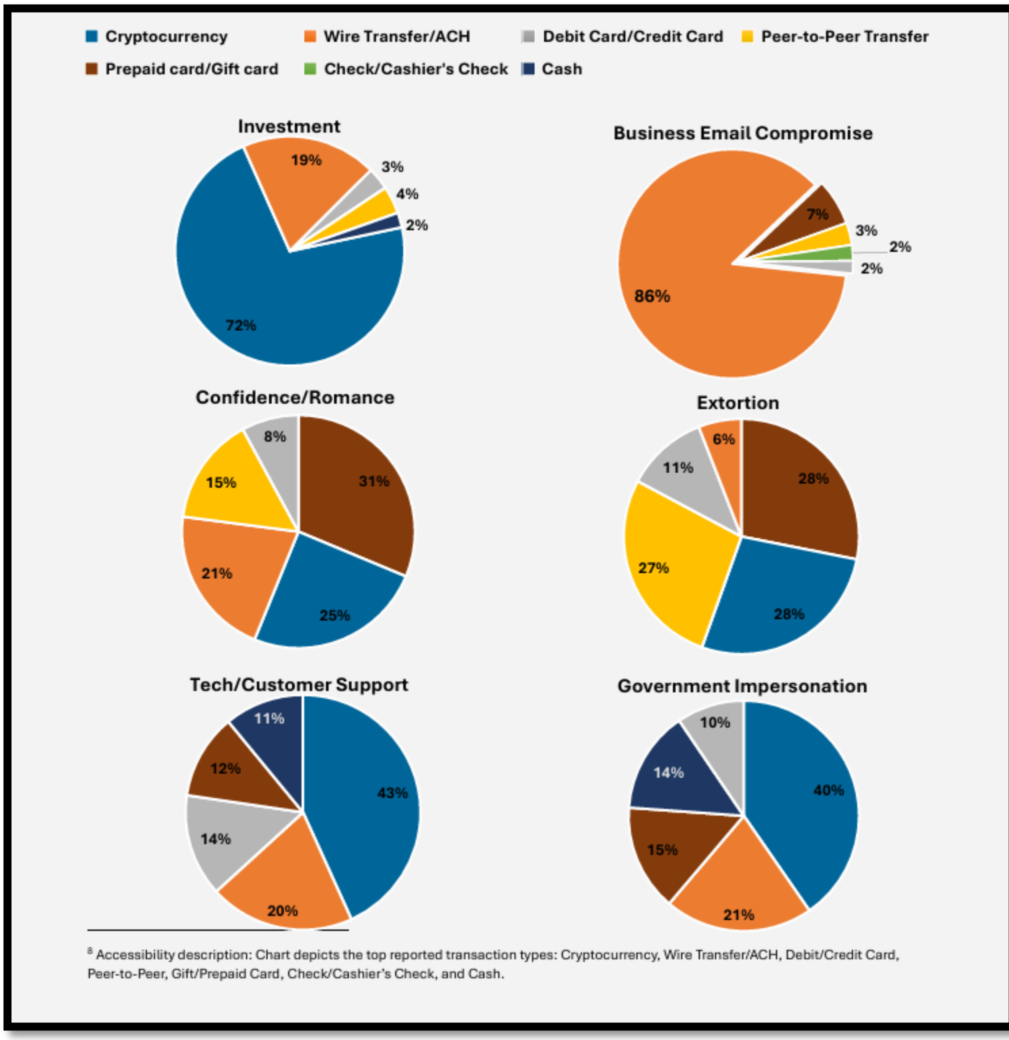
Fraudsters and scammers have also begun exploiting modern payment methods. Faster payment methods, such as wire transfers and payment applications, have allowed fraudsters and scammers to complete their schemes more quickly and have improved their ability to remove the funds from the financial system before they can be reclaimed by financial institutions.[329] Further, many scammers have started demanding payment in digital assets, with the FTC identifying $1.78 billion in payments to fraudsters and scammers made using digital assets in 2025.[330] Notably, blockchain analytics show that illicit activity only accounts for at most one percent of digital asset transaction volume.[331] Although digital asset ATMs are legitimate mechanisms for purchasing or transferring digital assets, fraudsters increasingly direct individuals to use digital

---

[324] Pieter Arntz, *How AI Made Scams More Convincing in 2025*, MALWAREBYTES LABS (Jan. 2, 2026), https://www.malwarebytes.com/blog/news/2026/01/how-ai-made-scams-more-convincing-in-2025; U.S.-CHINA ECON. & SEC. REVIEW COMM'N, PROTECTING AMERICANS, *supra* note 322, at 3-4.
[325] *Safeguarding Main Street*, *supra* note 44 (statement of Ms. Jilenne Gunther, Nat'l Dir., BankSafe Initiative).
[326] U.S.-CHINA ECON. & SEC. REVIEW COMM'N, PROTECTING AMERICANS, *supra* note 322, at 3-4.
[327] *Id.*
[328] *See* Benjamin Gorman, *AI Scams: What are They and How Can You Avoid Them?*, NORTON (May 6, 2026), https://us.norton.com/blog/ai/ai-scams.
[329] ASPEN INST., UNITED WE STAND, *supra* note 282.
[330] FTC Fraud Reports Data, *supra* note 11.
[331] *2026 Crypto Crime Report Introduction*, CHAINALYSIS: BLOG (Jan. 8, 2026), https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/.

asset ATMs to remit payment due to the ability to move money through these systems faster than traditional payment methods.[332]

Exhibit K: Reported Fraud & Scam by Payment Method[333]



The rapid growth of digital asset ATM scams is driven, in part, by the current regulatory gap that existing frameworks do not fill. While ATM operators are classified as money services businesses under guidance from the Financial Crimes Enforcement Network (FinCEN) and are subject to BSA obligations,[334] there are no standard daily deposit caps on digital asset ATM

---

[332] FIN. CRIMES ENF'T NETWORK, FIN-2025-NTC1, FINCEN NOTICE ON THE USE OF CONVERTIBLE VIRTUAL CURRENCY KIOSKS FOR SCAM PAYMENTS AND OTHER ILLICIT ACTIVITY 5-6 (2025).
[333] FBI 2025 INTERNET CRIME REPORT, *supra* note 25, at 9.
[334] FIN. CRIMES ENF'T NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 1 (2013), *available at* https://www.fincen.gov/system/files/shared/FIN-2013-G001.pdf; FIN. CRIMES ENF'T NETWORK, FIN-2025-NTC1, *supra* note 332, at 3.

transactions.[335] FinCEN has warned that illicit activity risks are heightened when operators fail to implement appropriate anti-money laundering controls, customer due diligence, and other compliance measures.[336] Enactment of legislation, such as the *CLARITY Act*, would provide the regulatory framework necessary to impose meaningful safeguards.[337]

3. *Communication Technology*

The growth of anonymous online messaging platforms has empowered fraudsters and scammers worldwide. [338] Encrypted messaging platforms Telegram and WhatsApp now boast over one billion and 3.3 billion users, respectively.[339] They offer features that facilitate illicit activity while providing a target-rich environment for bad actors.[340] Fraudsters and scammers therefore prefer to operate on these platforms and act quickly to move victims into this scheme-friendly environment. [341] When convincing victims to move to an anonymous messaging platform, criminals use a variety of pretexts; one victim described meeting a scam account on a dating app, the operator of which immediately suggested moving the conversation to WhatsApp and deleting the dating app to "focus on getting to know each other."[342] Other schemes pose as exclusive digital asset trading groups, where victims click through ads on social media platforms regarding digital asset investments before being prompted to join Telegram or WhatsApp groups.[343] Whatever the excuse, once a victim is on an anonymous messaging platform, fraudsters and scammers take advantage of the apps' features to progress the scheme.[344]

Telegram and WhatsApp offer users enhanced anonymity through features like end-to-end chat encryption.[345] Telegram offers even more robust anonymity with features like phone number masking and secret chats.[346] End-to-end encryption denies access to chatlogs to all outside parties, making it more difficult for law enforcement to acquire and examine evidence and locate perpetrators.[347] Phone number masking allows criminals to obscure their real phone number or sign up with disposable numbers, making tracing them exceedingly difficult.[348] Secret chats are set to delete themselves after a given duration, further obscuring evidence of illicit

---

[335] *How Does a Crypto ATM Work? Fees, Limits, and Taxes*, LEGALCLARITY (Mar. 6, 2026), https://legalclarity.org/how-does-a-crypto-atm-work-fees-limits-and-taxes/.
[336] A.J.S. Dhaliwal et al., *FinCEN Warns Financial Institutions of Illicit Activity at Crypto Kiosks*, JDSUPRA (Aug. 8, 2025), https://www.jdsupra.com/legalnews/fincen-warns-financial-institutions-of-6483022/; FIN. CRIMES ENF'T NETWORK, FIN-2025-NTC1, *supra* note 332, at 3.
[337] H.R. 3633 Tit. II, § 205.
[338] U.S.-CHINA ECON. & SEC. REVIEW COMM'N, CHINA'S EXPLOITATION OF SCAM CENTERS, *supra* note 18, at 2.
[339] Djordjevic, *supra* note 28; Rohit Shewale, *WhatsApp Users Worldwide (2026): Adoption, and Key Stats*, RESOURCERA (Feb. 26, 2026), https://resourcera.com/data/social/whatsapp-users/.
[340] Djordjevic, *supra* note 28.
[341] U.S.-CHINA ECON. & SEC. REVIEW COMM'N, CHINA'S EXPLOITATION OF SCAM CENTERS, *supra* note 18, at 2.
[342] Rebane & Watson, *supra* note 8.
[343] Stelian, *Fake AI Crypto Signal Group Scam on WhatsApp and Telegram*, MALWARETIPS (Aug. 14, 2023), https://malwaretips.com/blogs/fake-ai-crypto-signal-groups-scam-on-whatsapp-and-telegram/.
[344] Djordjevic, *supra* note 28.
[345] Michael Bordash, *The Dark Side of End-to-End Encryption: Scams in 2025*, LINKEDIN (Feb. 10, 2025), https://www.linkedin.com/pulse/dark-side-end-to-end-encryption-scams-2025-michael-bordash-5fsne.
[346] Djordjevic, *supra* note 28.
[347] Bordash, *supra* note 345.
[348] *FAQ,* TELEGRAM, https://telegram.org/faq#q-what-makes-telegram-groups-cool (last visited June 4, 2026).

activity.[349] All of these features allow fraudsters and scammers to act with a greater degree of freedom in perpetrating their schemes, covering their tracks with relative ease or, if executed properly, leaving no tracks at all.[350]

The scale of these messaging networks enables mass fraud and scam activity.[351] For instance, Telegram supports group chats containing up to 200,000 members; through these channels a single post or suspicious link can reach a large audience instantly.[352] Moreover, illegitimate posts and fraudulent links can appear to be entirely legitimate when supported by bot network traffic that fabricate reactions, interaction, and engagement.[353]

The potent combination of anonymity-enhancing features and a massive user base can lead to life-shattering outcomes; a father in New Jersey was recently scammed out of his entire life savings after an account presenting itself as a potential romantic partner convinced him to connect on Facebook, message on WhatsApp, and invest in a fraudulent digital asset scheme.[354] Elsewhere, an Orange County resident lost over $2.3 million in a romance scam in which she communicated with the scammer via WhatsApp.[355] Further, the U.S. Securities and Exchange Commission (SEC) has recently charged multiple digital asset trading platforms and investor clubs for defrauding more than $14 million from retail investors who were enticed into joining WhatsApp "investing" groups.[356]

Additionally, Telegram and WhatsApp facilitate communication and coordination of fraud and scam activity by serving as a meeting place for fraudsters, scammers, and other varieties of criminals.[357] Through Telegram, these criminals will buy and sell victims' personally identifiable information (PII), including social security and other identification information, serving as a vital marketplace for criminals and scammers across the globe.[358] These criminals will also share advice with each other on how to improve their fraud and scam efforts.[359]

A WHOLE-OF-ECOSYSTEM APPROACH IS NEEDED

As evidenced above, the threat of fraud and scams is multi-pronged—criminals leverage multiple vectors and exploit any means possible to steal Americans' savings. Although financial

[349] Djordjevic, *supra* note 28.
[350] *Id.*
[351] *Id.*
[352] *Id.*; *FAQ,* TELEGRAM, https://telegram.org/faq#q-what-makes-telegram-groups-cool (last visited June 4, 2026).
[353] Djordjevic, *supra* note 28.
[354] Rebane & Watson, *supra* note 8.
[355] *Orange County Woman Loses $2.3 Million to Romance Scam*, CBS NEWS (May 11, 2023), https://www.cbsnews.com/losangeles/news/orange-county-woman-loses-to-romance-scam-2-3-million/.
[356] Press Release, Sec. & Exch. Comm'n, SEC Charges Three Purported Crypto Asset Trading Platforms and Four Investment Clubs with Scheme That Targeted Retail Investors on Social Media (Dec. 22, 2025), https://www.sec.gov/newsroom/press-releases/2025-144-sec-charges-three-purported-crypto-asset-trading-platforms-four-investment-clubs-scheme-targeted.
[357] Julia Dickson et. al, *Cyber Scamming Goes Global: Unveiling Southeast Asia's High-Tech Fraud Factories*, CTR FOR STRATEGIC & INT'L STUDIES (Dec. 12, 2024), https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories.
[358] Teshar Subhra Dutta, *Cybercriminals Use Telegram Channels to Sell Verified Bank and Fintech Mule Accounts*, CYBER SEC. NEWS (May 25, 2026), https://cybersecuritynews.com/cybercriminals-use-telegram-channels/.
[359] U.S.-CHINA ECON. & SEC. REVIEW COMM'N, PROTECTING AMERICANS, *supra* note 322, at 4.

losses are typically realized within the financial system, fraud and scams regularly originate outside it, with modern fraud and scams frequently starting though tech platforms and telecommunications networks. And while some fraudsters and scammers are physically within the United States, they are more commonly finding refuge in foreign jurisdictions—particularly Southeast Asia.[360] As the above data shows, criminals do not discriminate based on geography, age, gender, race, political affiliation, or other characteristic. Their only intent is to deprive hard-working individuals and businesses of their money.

These crimes are of such a magnitude and complexity that no one person, company, or agency can tackle the problem alone.[361] As the American Bankers Association (ABA) identified, "the scope and scale of this challenge is far too large for one bank – or even one industry – to tackle alone."[362] Rather, it will require a "whole-of-ecosystem" approach.[363] Those sectors that criminals target or exploit—particularly telecommunications, messaging, social media, technology, and financial services—must work independently and collaboratively, including with law enforcement and government counterparts across local, state, and federal levels.[364]

Combating these crimes will also require a multi-pronged solution. Stakeholders at every level must develop and implement both proactive and, where necessary, reactive tools to counter, dissuade, and disrupt fraud and scams. Such tools and efforts must not simply focus on recompensation—at that point, individuals have already been victimized and their money stolen, with little chance of recovery. Rather, both public and private sector stakeholders must do their part to enact policies and procedures aimed at eliminating opportunities for bad actors to perpetrate these crimes—stopping crimes before they occur.

PUBLIC AND PRIVATE SECTOR ENTITIES HAVE TAKEN SOME STEPS TO MITIGATE THE RISE IN FRAUD AND SCAMS

Throughout the Committee's work, it has become clear that stakeholders across the public and private sectors recognize the threat of financial fraud and scams. Interest groups and non-profits have been sounding the alarm over the continued rise in both number of victims and monetary loss. Many private sector companies and public agencies—at the local, state, and federal level—are currently investing not only in systems and processes designed to identify and stop fraud and scams, but also in innovative tools and solutions.[365] Industry is also working to better integrate efforts, creating new alliances and groups focused on information sharing. The Trump Administration, for its part, has also sought to prioritize addressing these crimes, issuing Executive Orders (EOs) and creating task forces focused on combating fraud and scams pose.

[360] Dickson et al, *supra* note 357.
[361] *See* briefings with Committee Republican staff (notes on file with the Committee).
[362] *Chair's View: Taking the fraud fight to the trenches*, ABA BANKING JOURNAL (Aug. 13, 2025), https://bankingjournal.aba.com/2025/08/chairs-view-taking-the-fraud-fight-to-the-trenches/.
[363] ASPEN INST., UNITED WE STAND, *supra* note 282, at 10
[364] *Id.* at 8.
[365] *See generally* briefings with Committee Republican staff (notes on file with the Committee); *Fighting Fraud on the Front Lines*, *supra* note 43; *Fraud in Focus*, *supra* note 42. *See also* ASPEN INST., UNITED WE STAND, *supra* note 282, at 10.

A. Examples of Innovative Efforts from Private Sector

Stakeholders across the financial services, technology, and telecommunications industries are taking action to combat fraud and scams. Financial institutions, for example, are currently investing heavily in fraud detection, mitigation, and customer protection.[366] Even where a financial institution does not have a legal responsibility to reimburse customers, financial institutions are still motivated to implement proactive measures to protect the customer experience in a highly competitive banking environment. Those customers increasingly expect their financial institutions to protect them against scams and respond positively when they make these investments.[367] In fact, a study by Notre Dame Professor Vamsi Krishna Kanuri found that when banks dedicate resources to identifying the perpetrators of customer scams, their customers are much more likely to remain loyal to that financial institution, even when compared with those customers who never experienced scams at all.[368]

The same is true of the other industries through which many fraud schemes and scams originate, particularly telecommunications and social media. Currently, these industries face little-to-no legal liability for allowing fraud and scams to operate via their services. However, they are subject to customer satisfaction. If customers believe these platforms are heavily prone to perpetuate fraud and scams, customers may think twice before using the services. Further, companies do not want their brands associated with fraud and scams. Thus, telecommunications, social media, and technology companies are increasingly adopting tools and tactics to address fraud and scams.

Below are some of the key innovative tools and solutions that these companies are adopting to reduce the volume of fraud and scams targeting Americans.

1. *Introduction of Friction & Leveraging of Innovative Solutions*

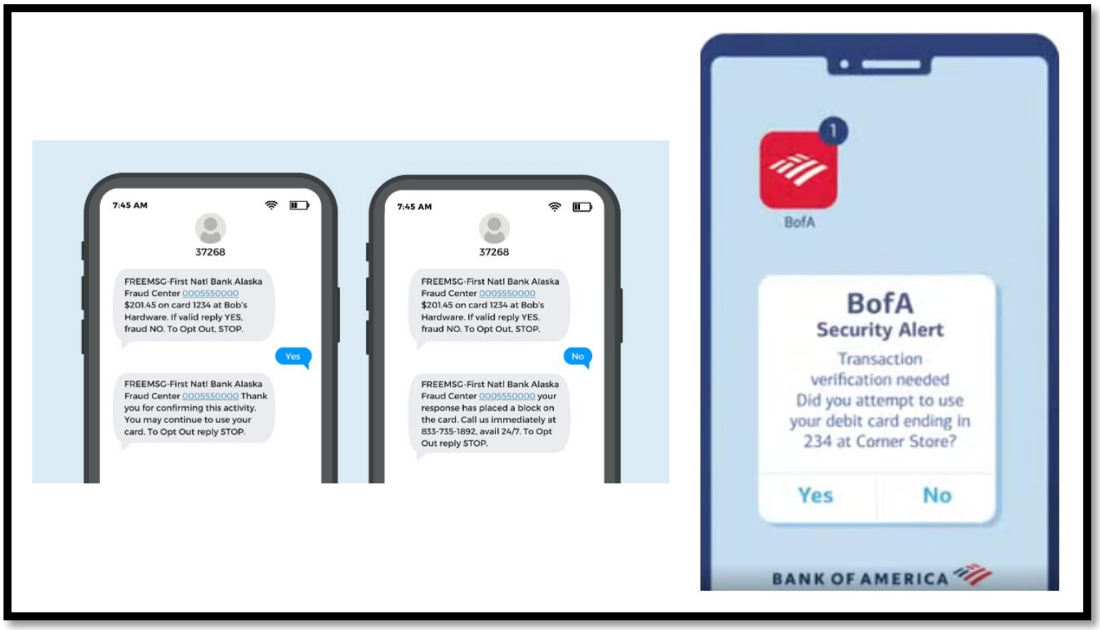
As fraud and scams grow in scale and sophistication, companies within the industries most impacted have worked to develop layered defenses designed to slow, detect, and block fraudsters. Banks, telecommunications providers, and social media companies are each deploying a combination of behavioral technology and regulatory compliance measures in what has become an arms race against increasingly capable criminals. In fact, nearly every stakeholder with whom Committee staff spoke described efforts they have taken to introduce “friction” into their systems.[369] Friction is designed to slow an interaction or financial transaction down without negatively impacting the consumers’ experience so significantly that it drives the individual to use alternative payment platforms.[370]

---

[366] GAO-24-107107, *supra* note 30.
[367] Debbie Cobb, *5 Scam Protections Customers Want from their Bank,* FICO Blog (May 3, 2023), https://www.fico.com/blogs/5-scam-protections-customers-want-their-bank.
[368] Shannon Roddel, *Banks that identify fraudsters increase loyalty, retain more defrauded customers than others who were never compromised*, NOTRE DAME NEWS (Sep. 22, 2025), https://news.nd.edu/news/banks-that-identify-fraudsters-increase-loyalty-retain-more-defrauded-customers-than-others-who-never-were-compromised/.
[369] Briefings with Committee Republican staff (notes on file with the Committee).
[370] Briefings with Committee Republican staff (notes on file with the Committee).

Financial Institutions. Financial institutions have long understood that deliberate friction—such as small, targeted delays and verification steps—is one of the most effective tools against fraud. For example, most financial institutions have introduced fraud alerts and real-time transaction notifications to help flag potentially suspicious transactions before the customer sends money.[371] These efforts are particularly robust in the peer-to-peer space, where financial institutions frequently use click-through pop-ups to warn customers about fraud risks, require attestations confirming the customer knows the recipient, send confirmation messages, and implement safeguards to block payments to recipients that customers met on social media.[372]

Exhibit L: Examples of Financial Institution Security Alerts[373]



Financial institutions are also prioritizing data analytics and real-time monitoring. Practically every stakeholder in the financial sector detailed technological systems they use to monitor for and flag suspicious transactions.[374] According to Block's Chief Risk Officer, Brian Boates, Cash App decreased its "Confirmed Scam Rate" by nearly 70 percent between December 2024 and May 2025 "by fine tuning [their] systems to maintain healthy warning rates, block rates, and false positive metrics, ensuring [they are] stopping bad actors without creating

[371] *Fraud in Focus*, *supra* note 42 (testimony of Paul Benda, Am. Bankers Ass'n).

[372] Briefings with Committee Republican staff (notes on file with the Committee); Tania Luviano-Hurwitz, *Why your bank may block your next Zelle Payment*, NBC SAN DIEGO (Jan. 12, 2026), https://www.nbcsandiego.com/nbc-7-responds-2/zelle-banks-security-measures/3959840/.

[373] *Fraud Prevention Text Alerts*, FIRST NAT'L BANK OF ALASKA, https://www.fnbalaska.com/premium-enfact-text-alerts/ (last visited June 3, 2026) (showing how some banks will send their customers texts when they flag suspicious or unusual activity and ask the customer to confirm, via text, whether the suspicious activity was valid or not); Bank of America, FACEBOOK (Jan. 3, 2022), https://www.facebook.com/BankofAmerica/videos/bank-of-america-security-alerts/278302794362397/.

[374] Briefings with Committee Republican staff (notes on file with the Committee).

unnecessary hurdles for [their] customers."[375] Stakeholders are also training branch and call center employees to recognize and prevent fraud and scams.[376] Interventions from trusted frontline staff can be particularly powerful in disrupting the influence that fraudsters and scammers exert over consumers.[377]

One key issue these institutions deal with is how to carefully calibrate friction such that it stops bad actors without alienating legitimate customers.[378] Behind the scenes, financial institutions and payment processors have also been quietly overhauling their modeling of customer behavior.[379] Historical fraud alert systems relied on static rules—for example, flagging purchases outside a cardholder's zip code or charges above certain thresholds—but sophisticated criminals learned those rules and simply worked around them by spoofing locations or keeping transaction amounts just below trigger thresholds.[380] Newer systems, instead, build detailed behavioral models of individual customers, which provides much richer data and makes fraud easier to detect.[381] One stakeholder referenced their use of BioCatch, technology that "analyz[es] human digital physical and cognitive behavior" to allow the stakeholder to develop known customer profiles, which in turn informs flags for suspicious behavior.[382] As another example, Visa recently established the Visa Scam Disruption (VSD) practice, which "identified more than $1 billion in fraud attempts" in just its first year of creation.[383] VSD, which is housed under Visa's Payment Ecosystem Risk and Control Department and which has saved victims more than "$350 million across dozens of scams [in 2024]," employs a cross-disciplinary team, including engineers, AI developers, former law enforcement, and beyond, engages in proactive investigations, and leverages generative AI tools to "enable correlation and graphing analysis to identify complex relationships and parse through mass amounts of data to identify true positive and impactful scam activity."[384] The practical upshot for customers is that consistency matters: using the same device, maintaining regular login patterns, and allowing the bank to observe routine behavior all improve the model's accuracy and reduce false positives over time.

Telecommunications. As described above, telephone and wireless carriers sit at the chokepoint through which most fraud and scam communications must pass, giving them unique leverage—and unique responsibility—in the fight. Given the staggering number of robocalls and spam texts, wireless providers have introduced methods to block such calls and successfully

---

[375] *Making Money Moves Safer: Our Progress in Protecting Cash App Customers*, BLOCK (May 6, 2025), https://block.xyz/inside/progress-in-protecting-cash-app-customers.
[376] Judith Sears, *Fighting Fraud with Tech and Training*¸ INDEP. BANKER (Oct. 1, 2025), https://www.independentbanker.org/w/fighting-fraud-with-tech-and-training.
[377] *Id.*
[378] Briefings with Committee Republican staff (notes on file with the Committee).
[379] Briefings with Committee Republican staff (notes on file with the Committee).
[380] *Why Bank Fraud Alerts Got Smarter in 2026—And What You'll Actually Notice*, DOWNBEACH (May 1, 2026), https://downbeach.com/news/2026/may/01/why-bank-fraud-alerts-got-smarter-in-2026-and-what-youll-actually-notice/.
[381] *Id.*
[382] Briefings with Committee Republican staff (notes on file with the Committee); *Our Story*, BIOCATCH, https://www.biocatch.com/about-biocatch.
[383] Paul Fabara, *Protecting consumer payments, one billion dollars at a time*, VISA (Sep. 25, 2025), https://corporate.visa.com/en/sites/visa-perspectives/security-trust/scam-disruption-hits-one-billion-milestone.html.
[384] Press Release, Visa, Visa Unveils its Scam Disruption Practice, Helping Protect Consumers and the Financial Ecosystem Globally (Mar. 11, 2025), https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.21286.html.

blocked 55 billion spam and scam robotexts in 2024.[385] Many carriers also flag or block approximately 45 billion scam calls per year.[386] Various stakeholders in the telecommunications industry informed Committee staff of technology they have implemented to address fraudulent and scam calls.[387] As one example, Apple included several features in the operating system it introduced in 2025, iOS 26. In this update, Apple added a call screening feature that allows users to block specific callers and "change [their] setting[s] to automatically identify, screen, filter, and block unknown and spam calls."[388] Users can choose to send calls from unknown callers direct to voicemail, or require unknown callers to provide their name and the reason for their call; once this information is provided a user's phone will ring and share the caller's response, allowing the user to decide whether to answer the call.[389] iOS 26 also includes a similar feature for screening, filtering, reporting, and blocking text messages from unknown senders.[390] Additionally, Apple introduced a security update that it claims will provide additional, robust defenses against malicious spyware attacks, limiting cybercriminals ability to skim personal information through these attacks.[391]

A central pillar of the American telecommunications industry's technical response is the Secure Telephone Identity Revisited (STIR)/Signature-based Handling of Asserted Information using ToKENs (SHAKEN) protocol—a caller authentication framework mandated by the FCC under the *2019 Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act* (Pallone-Thune TRACED Act).[392] STIR/SHAKEN enables originating providers to digitally sign calls, allowing terminating providers to verify caller identity.[393] However, stakeholders noted that implementation remains a work in progress, as even though large carriers have achieved strong adoption, smaller carriers lag significantly, creating gaps that fraudsters exploit.[394]

Members of the telecommunications industry also informed the Committee of efforts they are undertaking to address the rise in fraudulent and spam text messages. Stakeholders informed Committee staff that they are working hard to limit obvious non-human contacts. As one stakeholder noted, "a human clearly cannot send 10,000 messages at once—making it generally easier to determine human versus not human."[395] As one example, a stakeholder

---

[385] Erika Kinetz & Juliet Linderman, *Congressional Committee Asks Telecoms to do More to Prevent Scams as Losses Surge*, WASHINGTON TIMES (May 21, 2026), https://www.washingtontimes.com/news/2026/may/21/congressional-committee-requests-telecoms-prevent-scams-losses-surge/.
[386] *Id.*
[387] Briefings with Committee Republican staff (notes on file with the Committee).
[388] *Screen and block calls on iPhone*, APPLE, https://support.apple.com/guide/iphone/screen-and-block-calls-iphe4b3f7823/26/ios/26 (last visited Dec. 2, 2025).
[389] *Id.*
[390] *Id.*
[391] *Apple Security Engineering and Architecture, Memory Integrity Enforcement: A complete vision for memory safety in Apple devices*, APPLE (Sep. 9, 2025), https://security.apple.com/blog/memory-integrity-enforcement/.
[392] *See* 47 U.S.C. § 227b.
[393] *Combating Spoofed Robocalls with Caller ID Authentication*, FED COMMS. COMM'N, https://www.fcc.gov/call-authentication.
[394] Briefings with Committee Republican staff (notes on file with the Committee).
[395] Briefings with Committee Republican staff (notes on file with the Committee).

described technology they have implemented that analyzes volume metrics and key words across messages that indicate fraud and scams.[396]

Many telecommunications carriers have implemented firewall filters and detection systems to help prevent spam text messages from reaching customers.[397] For those messages that get through, many of the carriers allow customers to report spam messages by "reporting" the texts or forwarding them to 7726 and 7727, commercial short codes operated by mobile carriers.[398] The carriers' systems then capture technical metadata. Carriers can use this information to improve their internal filters, but because the information is anonymized, carriers can also share the information with other entities.[399]

Social Media & Technology. Social media platforms present a particular challenge because their open, ad-supported business models have historically created incentives that can run counter to aggressive fraud prevention. Scammers exploit these platforms to locate victims, place fraudulent advertisements, and build fake personas that lure people into investment traps or romance scams.[400] Multi-channel scams—where victims are lured from social media into encrypted chats and fraudulent payment pages—are expected to become the dominant scam pattern in 2026, with AI chatbots and deepfake companions increasingly blurring the line between real and synthetic interactions.[401]

Advertisements present a particular challenge, as many current fraud and scams begin through fraudulent advertisements on Google, Facebook, Instagram, TikTok, and other platforms. As explained above, such ads may impersonate trusted brands, offer goods or services that do not exist, or promote misleading deals.[402] The tech platforms have a monetary incentive to keep such advertisements up, given that each platform generates billions of dollars from hosting advertisements. In 2024, for example, Google advertising generated more than $264 billion in revenue.[403] As another example, Meta generates "substantially all of [its] revenue from selling advertising placements on [its] family of apps to marketers[.]"[404] In 2025, Meta generated

---

[396] Briefings with Committee Republican staff (notes on file with the Committee).
[397] Shara Agarwal et al., *An Overview of 7726 User Reports: Uncovering SMS Scams and Scammer Strategies*, ARXIV (Nov. 10, 2025), https://arxiv.org/html/2508.05276v2; briefings with Committee Republican staff (notes on file with the Committee).
[398] Adam Grucela, *Where does the 7727 text message come from?*, INCOGNI, https://blog.incogni.com/7727-text-message/.
[399] *Id.*; Agarwal et al., *supra* note 397; briefings with Committee Republican staff (notes on file with the Committee).
[400] *See* Public Service Announcement Alert No. I-120324-PSA, Fed. Bureau of Investigation, Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud (Dec. 3, 2024), https://www.ic3.gov/PSA/2024/PSA241203.
[401] *See* TRENDMICRO, 2026 SCAM PREDICTIONS: HOW AI AND EMOTION ARE RE-ENGINEERING GLOBAL SCAMS (2025), *available at* https://newsroom.trendmicro.com/2025-12-03-Trend-Micro-Predicts-2026-as-the-Year-Scams-Become-AI-Driven,-AI-Scaled,-and-Emotion-Engineered.
[402] *Social Media Scam Ads are Everywhere. Here's How to Spot Them*, CONSUMER THREATS (Feb. 10, 2026), https://www.idx.us/knowledge-center/social-media-scam-ads-are-everywhere-heres-how-to-spot-them.
[403] Alphabet Inc., Annual Report (Form 10-K) 36 (Jan. 31, 2025), *available at* https://www.sec.gov/Archives/edgar/data/1652044/000165204425000014/goog-20241231.htm.
[404] Meta Platforms, Inc., Annual Report (Form 10-K) 6 (Jan. 29, 2025), *available at* https://www.sec.gov/Archives/edgar/data/1326801/000132680125000017/meta-20241231.htm.

nearly $201 billion in revenue.[405] In the case of advertisements, the platform's customer is the advertiser.

Stakeholders in this space stressed that they are working to address fraudulent ads and caveated that they have no incentive to have fraudulent advertisements on their platforms.[406] According to these stakeholders, fraudulent advertisements ruin the user experience, which runs counter to business incentives.[407] As evidence of their efforts to counter fraudulent advertisements, Google created the Limited Ad Serving program, which "limit[s] impressions of ads that have a higher potential of causing abuse or a poor experience for users."[408] Google also prohibits uncertified advertisers from serving certain ads.[409] Google's limited ad serving functions as a get-to-know-you process and therefore primarily affects new advertisers. While Google "gets to know" the advertiser, the advertisers' "ad impressions may be limited" in certain scenarios.[410] Limited ad serving considers user feedback, prevalence of abuse, and industry trends "when determining if a particular scenario has a higher potential of causing abuse or creating a poor user experience[.]"[411] To determine whether an advertiser is qualified, Google reviews account attributes, user activity and reports, account maturity, ad format usage, history of policy-compliance, advertiser industry, and identity verification status.[412]

Both public accounts and many stakeholder conversations with Committee staff emphasized that Meta platforms are a major originator of fraud and scams.[413] The FTC estimated that victims lost more money to fraud and scams originating on Meta-owned platforms than on any other platform, with the cumulative losses across Facebook, WhatsApp, and Instagram exceeding the combined losses from text and email scams.[414] According to recent reports, internal company documents showed that Meta was aware it was profiting off of these schemes.[415] For example, internal documents allegedly show that Meta "projected late last year that it would earn about 10 percent of its overall annual revenue—or $16 billion—from running advertising for scams and banned goods[.]"[416] A December 2024 document also allegedly concluded that Meta "shows its platforms' users an estimated 15 billion 'higher risk' scam advertisements—those that show clear signs of being fraudulent—every day."[417] Further, internal

---

405 Press Release, Meta, Meta Reports Fourth Quarter and Full Year 2025 Results (Jan. 28, 2026), https://investor.atmeta.com/investor-news/press-release-details/2026/Meta-Reports-Fourth-Quarter-and-Full-Year-2025-Results/default.aspx.
406 Briefings with Committee Republican staff (notes on file with the Committee).
407 Briefings with Committee Republican staff (notes on file with the Committee).
408 *Limited ad serving, Advertising Policies Help*, GOOGLE, https://support.google.com/adspolicy/answer/13889491?hl=en (last visited Dec. 1, 2025).
409 *Id.*
410 *Id.*
411 *Id.*
412 *Id.*
413 Briefings with Committee Republican staff (notes on file with the Committee).
414 Div. of Consumer Response & Ops. Staff, *Reported Losses to Scams on Social Media Eight Times Higher than in 2020*, FED. TRADE COMM'N (Apr. 27, 2026), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2026/04/reported-losses-scams-social-media-eight-times-higher-2020.
415 Jeff Horwitz, *Meta is earning a fortune on a deluge of fraudulent ads, documents show*, REUTERS (Nov. 6, 2025), https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.
416 *Id.*
417 *Id.*

documents from 2025 reportedly show that Meta staff estimate "that the company's platforms were involved in a third of all successful scams in the [United States]."[418] Meta staff also reportedly acknowledged that it is easier to advertise scams on Meta products versus Google.[419] Yet, Meta continued to host and promote such ads, opting to "only [ban] advertisers if [Meta's] automated systems predict the marketers are at least 95 [percent] certain to be committing fraud."[420] Even where stakeholders agreed that Meta removed scam ads, many argued that the company moved too slow in doing so.[421]

Meta has pushed back on the characterizations above, deriding the public reports as "present[ing] a selective view that distort[ed] Meta's approach to fraud and scams."[422] Per Meta, some of the numbers were "rough and overly-inclusive" and ultimately determined to be lower.[423] In both public reporting and in conversations with Committee staff, Meta argued that it has made—and continues to make—robust efforts to counter fraudulent advertisements and content on its platform using a combination of "AI enabled defenses" and expanded advertiser verification.[424] On the former, Meta recently announced efforts to better address "friending" and messaging from unknown contacts, including working with satellite providers through which scammers in foreign countries are posing as U.S.-based individuals.[425] Importantly, Meta is also purportedly partnering with law enforcement to address scam center-related issues, including having recently participated in a global law enforcement operation that disabled over 150,000 accounts linked to scam networks and contributed to 21 arrests by the Royal Thai Police.[426]

On advertisements, the company publicly announced that it aims to have verified advertisers drive 90 percent of ad revenue by the end of 2026, up from 70 percent today.[427] Nevertheless, Meta has acknowledged that it does not require universal advertiser verification.[428] It argued that certain advertisers may only post locally or advertise such a minimal amount that they should not be considered "high-risk" to warrant verification.[429] Meta also noted that other case studies have shown that universal verification is not a silver bullet to address fraudulent

---

418 *Id.*
419 *Id.*
420 *Id.*
421 Briefings with Committee Republican staff (notes on file with the Committee); SCAMBOOK: HOW META HELPS MEDICARE SCAMMERS TARGET SENIORS, CTR. FOR COUNTERING DIGITAL HATE 12 (2026), https://counterhate.com/wp-content/uploads/2026/05/Scambook_CCDH_Final.pdf.
422 Horwitz, *supra* note 415.
423 *Id.*
424 News Release, Meta, Fighting Scammers and Protecting People with New Technology and Partnerships (Mar. 11, 2026), https://about.fb.com/news/2026/03/fighting-scammers-protecting-people-with-new-technology-and-partnerships/ [hereinafter Meta, Fighting Scammers]; News Release, Meta, Meta Launches New Anti-Scam Tools, Deploys AI Technology to Fight Scammers and Protect People (Mar. 2026), https://about.fb.com/news/2026/03/meta-launches-new-anti-scam-tools-deploys-ai-technology-to-fight-scammers-and-protect-people/amp/ [hereinafter Meta, Launches New Anti-Scam Tools]; briefings with Committee Republican staff (notes on file with the Committee).
425 Briefing with Committee Republican staff (notes on file with the Committee).
426 Meta, Fighting Scammers, *supra* note 424.
427 Meta, Launches New Anti-Scam Tools, *supra* note 424; briefings with Committee Republican staff (notes on file with the Committee).
428 Briefing with Committee Republican staff (notes on file with the Committee).
429 Briefing with Committee Republican staff (notes on file with the Committee).

advertisements.[430] Such responses have done little to assuage concerns voiced by the American public, stakeholders, and Members of Congress regarding their lack of prioritization to address fraudulent advertisements. As public reports have described, even where fraudulent advertisements are reported on multiple occasions, the advertisements often remain live, and the advertisers behind them remain on the platform, allowing the criminals to victimize more individuals.[431]

2. *Private Industry Lawsuits*

Although much of the focus of private stakeholders is currently on internal tools to combat fraud and scams, two companies have recently sought to draw further attention to this issue through private lawsuits aimed at cracking down on criminals located abroad. The lawsuits reflect a tactic that companies have periodically used: since criminal ecosystems often operate in countries that do not cooperate with U.S. law enforcement, the companies wage court battles to obtain legal authority to seize and dismantle the infrastructure on which criminals rely—even when the criminals themselves remain out of reach.

Google has pursued three separate but related lawsuits against scam operators. In November 2025, Google filed a lawsuit against Lighthouse, a primarily China-based organization that Google alleges runs a phishing-as-a-service kit business.[432] Lighthouse reportedly "includes hundreds of templates for fake websites, domain set-up tools for those fake websites, and other features designed to dupe victims into believing they are entering sensitive information on a legitimate website."[433] According to public reporting, "[t]he texts usually contain malicious links to a fake website designed to steal victims' sensitive financial information, including Social Security numbers, banking credentials and more."[434] These texts take many forms, including but not limited to "fake fraud alert[s], delivery update[s], unpaid government fee notification[s], or other seemingly urgent texts."[435] One example includes E-ZPass scams,[436] where an individual receives a text that they have an unpaid toll fee. Google alleged the Lighthouse operation harmed more than one million victims across 120 countries, stealing between 12.7 million and 115 million credit cards in the United States alone—

---

430 Briefing with Committee Republican staff (notes on file with the Committee).
431 *Cf.* Lily Mae Lazarus, *Former Meta integrity chief says new report reveals 'disappointing' ad fraud epidemic at the social media giant*, FORTUNE (Dec. 15, 2025), https://fortune.com/2025/12/15/former-meta-integrity-chief-ad-fraud-epidemic-china-scams/; Alice Cullinane & Rebecca Woods, *Meta accused of letting AI sellers 'run rampant'*, BBC (Nov. 29, 2025), https://www.bbc.com/news/articles/c4gpz90d4q0o; *Meta Awash in Deepfake Scam Ads*, TECH TRANSPARENCY PROJECT (Oct. 1, 2025), https://www.techtransparencyproject.org/articles/meta-awash-in-deepfake-scam-ads.
432 Plaintiff's Complaint for Damages and Injunctive Relief 3, Google v. Does 1-25, Case 1:25-cv-09421 (S.D.N.Y. Nov. 12, 2025), *available at* https://www.courtlistener.com/docket/71900274/1/google-llc-v-does-1-25/. *See also* Jaures Yip, *Google sues cybercriminal group behind E-ZPass, USPS text phishing scams*, CNBC (Nov. 12, 2025), https://www.cnbc.com/2025/11/12/google-e-zpass-usps-text-scam-phishing-suit.html?msockid=2b25242999fa650235ab31e8985d64c0.
433 *Id.*
434 *Id.*
435 *Id.*
436 *Id.*

representing a fivefold increase in such attacks since 2020.[437] Per Google's General Counsel, "[t]he idea [behind the lawsuit] is to prevent its continued proliferation, deter others from doing something similarly, as well as protect both the users and brands that were misused in these websites from future harm."[438] As of December 1, 2025, the Southern District of New York granted a preliminary injunction against the defendants pending further proceedings.[439]

In December 2025, Google sued a Chinese cybercriminal group known as Darcula, which it accused of being responsible for a massive wave of scam text messages sent to Americans.[440] Darcula offers a program called Magic Cat, which contains an easy-to-use interface through which criminals with little technical skill can spam millions of phone numbers with links to fake websites that impersonate legitimate businesses and government agencies.[441] The criminals then steal the credit card numbers that victims enter.[442] Google alleged that Darcula and its associates stole "nearly 900,000 credit card numbers, including roughly 40,000 from Americans."[443] "From September to November alone, Google received more than 5,000 complaints from people who use Google Messages, the default text message app on Google Pixel phones, about Darcula scam texts."[444] With the lawsuit, Google aims to obtain legal standing for U.S. courts to allow Google to seize Darcula-operated websites, thereby hampering their operations.[445] As of April 7, 2026, the Southern District of New York entered a final default judgment in favor of Google, enabling Google to compel third parties to block web traffic to and from Darcula and/or associated domains, suspend services to Darcula and/or associated domains, and suspend any communication with Darcula and/or associated domains.[446]

Most recently, in June 2026, Google filed a lawsuit against unknown "foreign-based cybercriminals" who targeted Americans through AI-enabled phishing schemes.[447] According to the complaint, scammers were able to generate fraudulent websites that mimicked legitimate businesses and government agencies.[448] Google reported that it identified 9,000 fake websites and over one million fraudulent URLs connected to this group and that the group sent 2.5 million

---

[437] *Id. See also* Eric Revell, *Google Launches Dual Legal and Legislative Strategy to Combat International Cyber Scams*, FOX BUS. (Nov. 12, 2025), https://www.foxbusiness.com/technology/google-launches-dual-legal-legislative-strategy-combat-international-cyber-scams.
[438] Yip, *supra* note 432.
[439] *See* Preliminary Injunction Order, Google v. Does 1-25 Case 1:25-cv-09421 (S.D.N.Y. Dec. 1, 2025).
[440] *See* Plaintiff's Complaint for Damages and Injunctive Relief 1-3, Google v. Doe 1 a/k/a Yucheng Chang and Does 2-25, Case 1:25-cv-10440-JSR (S.D.N.Y. Dec. 17, 2025), *available at* https://www.courtlistener.com/docket/72046384/1/google-llc-v-doe-1/; Keivn Collier, *Google Sues Alleged Chinese Scam Group Behind Massive U.S. Text Message Phishing Ring*, NBCNEWS (Dec. 17, 2025), https://www.aol.com/articles/google-sues-alleged-chinese-scam-130000835.html.
[441] *Id.*
[442] *Id.*
[443] *Id.*
[444] *Id.*
[445] *Id.*
[446] Final Default Judgment for a Permanent Injunction 8-11, Google v. Doe 1 a/k/a Yucheng Chang and Does 2-25, Case 1:25-cv-10440-JSR (S.D.N.Y. Apr. 7, 2026), *available at* https://www.courtlistener.com/docket/72046384/44/google-llc-v-doe-1/.
[447] *See* Plaintiff's Complaint for Damages and Injunctive Relief 2, Google v. Does 1-25 (S.D.N.Y., June 2026), *available at* https://www.scribd.com/document/1049962658/Google-complaint-against-Outsider-phishing-enterprise.
[448] *See id.* at 2-3.

messages to Android users containing links to fraudulent website within just two weeks.[449] In that same period, Android users flagged 55,000 spam texts.[450]

Capital One has also sought to use private lawsuits to combat scam centers. In May 2026, the company sued ten unknown "persons and/or entities" associated with a large-scale robocall and telemarketing campaign for misusing trademarks for Capital One and Discover, a Capital One subsidiary.[451] According to the complaint, the defendants "use automated or prerecorded calls posing as representatives for the bank, and follow familiar scripts that warn of suspicious charges and ask the recipient to confirm the transaction or their identity."[452] Although Capital One's lawsuit seeks damages, the bank has stated publicly that its primary goal is to "expose and deter" bad actors and their associates.[453] As of May 27, 2026, the case is moving into discovery.[454]

3. *Cross-Industry, Private-Sector Partnerships*

The growing impact of fraud and scams and the realization that no one company or industry can solve the problem alone has driven the creation of many private cross-industry coalitions dedicated to sharing intelligence, pooling resources, and coordinating responses across sectors that have traditionally operated in silos. As various companies told Committee staff, private sector actors are beginning to establish informal partnerships across industries given that each company can only see an aspect of the overall fraud or scam.[455]

Beyond these informal relationships, industry is also working to establish more formal organizations and working groups aimed at combating fraud and scams. New organizations are popping up every day, but below are four key examples:

- *Global Anti-Scam Alliance (GASA).* GASA is the largest and most geographically broad of the cross-industry anti-fraud coalitions. Its mission is to reduce "the financial and emotional harm caused by scams worldwide through collaboration, research, and shared action."[456] With over 120 member organizations,[457] GASA functions as a convening platform for coordinated action across borders and sectors. Key member-companies include Microsoft, Gen Digital (the parent company of Norton and Avast), Google, Meta, Nasdaq Verafin, OpenAI, JPMorgan Chase (JPMC), Mastercard, and Visa, among many others.[458] GASA maintains regional chapters, including a North America chapter launched in 2025, and holds an annual Global Anti-Scam Summit (GASS) that convenes governments, regulators, law enforcement agencies, financial

[449] Halimah DeLaine Prado, *How We're Combatting AI Scams with Security, Legislation and More*, GOOGLE (June 12, 2026), https://blog.google/innovation-and-ai/technology/safety-security/combatting-ai-scams/.
[450] *Id.*
[451] Stephanie Dhue, *Capital One files lawsuit against alleged 'scam campaign' operators—for trademark infringement*, CNBC (May 13, 2026), https://www.cnbc.com/2026/05/13/capital-one-lawsuit.html.
[452] *Id.*
[453] *Id.*
[454] *See* Plaintiff's Order on Motion for Discovery, Capital One Financial Corp. v. John Does 1-10, 1:26-cv-01276 (E.D.V.A. May 27, 2026).
[455] Briefings with Committee Republican staff (notes on file with the Subcommittee).
[456] *About GASA – Our Mission*, GLOBAL ANTI-SCAM ALLIANCE, https://gasa.org/about (last visited June 24, 2026).
[457] *Our Members*, GLOBAL ANTI-SCAM ALLIANCE, https://gasa.org/members (last visited June 24, 2026).
[458] *Id.*

institutions, consumer protection bodies, and cybersecurity experts.[459] GASA also produces an annual "Global State of Scams" report, which aims to provide standardized cross-country data on scam prevalence and consumer harm, as well as reports on the state of scams in particular countries.[460]

- *Global Signal Exchange (GSE).* GSE is among the most technically ambitious cross-industry fraud initiatives to date. Described as the world's first global, multistakeholder, cross-sector clearinghouse for threat signals, the GSE was founded in 2024 by Oxford Information Labs Research (OXIL), Google, and GASA.[461] In July 2025, Microsoft and Meta joined as partners and data providers, bringing the total number of major collaborating organizations to over 30 global leaders.[462] In September 2025, the Singapore government also joined—the first and only publicly-reported government member to date.[463]

  GSE's core function is to enable partner organizations to securely share, analyze, and act on fraud-related data signals in real time.[464] As of January 2026, GSE was tracking one billion threat signals—a 2,400 percent increase from the 40 million signals tracked as of January 2025.[465] Membership is open to any organization interested in combating online scams, with membership tiers so entities can tailor their access to best fit their needs.[466] Organizations maintain their own data feeds and are encouraged to contribute to the collective effort.[467] The platform incorporates a feedback system that promotes swift reporting and quality control.[468]

- *Fraud Intelligence Reciprocal Exchange (FIRE).* Meta created FIRE to enable financial institutions to share threat intelligence directly with Meta, allowing the

---

[459] *Our Global Network*, GLOBAL ANTI-SCAM ALLIANCE, https://gasa.org/global-network/regions (last visited June 24, 2026); *Summits*, GLOBAL ANTI-SCAM ALLIANCE, https://gasa.org/events#summits (last visited June 24, 2026); briefing with Committee Republican Staff (notes on file with the Committee).

[460] *Knowledge Base – Reports*, GLOBAL ANTI-SCAM ALLIANCE, https://gasa.org/knowledge-base?content_group=318467252980&page=1 (last visited June 24, 2026).

[461] *About the Global Signal Exchange*, GLOBAL SIGNAL EXCH., https://www.globalsignalexchange.org/about (last visited June 24, 2026); briefings with Committee Republican Staff (notes on file with the Committee).

[462] News Release, Global Signal Exchange, Microsoft and Meta Join the Global Signal Exchange and the Collective Global Fightback Against Online Scams, Fraud and Abuse (July 30, 2025), https://www.globalsignalexchange.org/news/microsoft-and-meta-join-the-global-signal-exchange-and-the-collective-global-fightback-against-online-scams-fraud-and-abuse.

[463] Media Release, GovTech Singapore, First Government Agency to Join the GSE (Sep. 2, 2025), https://www.tech.gov.sg/media/first-government-agency-to-join-the-gse/.

[464] *Core Concepts*, GLOBAL SIGNAL EXCH. (Mar. 10, 2025), https://www.globalsignalexchange.org/docs/core-concepts; briefings with Committee Republican staff (notes on file with the Committee).

[465] Video posted by Emily Taylor, GLOBAL SIGNAL EXCH., *From 40 Million to 1 Billion Signals in 12-Months* (Feb. 3, 2026), https://www.globalsignalexchange.org/news/from-40-million-to-1-billion-signals-in-12-months.

[466] *Plans: Join the Fight Against Scams and Fraud*, GLOBAL SIGNAL EXCH., https://www.globalsignalexchange.org/plans (last visited June 24, 2026); *Frequently Asked Questions – Who is Eligible to Join, and More About Free and Sponsored Services*, GLOBAL SIGNAL EXCH., https://www.globalsignalexchange.org/docs/faq/who-is-eligible-to-join-and-more-about-free-and-sponsored-services (last visited June 24, 2026).

[467] *Platform Documentation*, GLOBAL SIGNAL EXCH., https://www.globalsignalexchange.org/docs/the-global-signal-exchange-platform (last visited June 24, 2026).

[468] *Id.*

company to use that information to identify and remove scam accounts across its network of applications.[469] The program was initially piloted in 2024 with UK banks, where it found success in the identification and removal of over 20,000 fraudulent accounts, including those associated with a large-scale concert ticket scam network targeting consumers in both the United Kingdom and the United States.[470] FIRE has since expanded to include more than 70 financial institutions worldwide.[471] The intelligence received through the program has directly resulted in the removal of tens of thousands of violating accounts, profiles, and pages.[472]

- *Industry Accord Against Online Scams and Fraud.* Most recently, in March 2026, eleven companies came together to launch the Industry Accord Against Online Fraud and Scams.[473] The seven-page agreement commits signatories to a set of voluntary principles and actions.[474] The Accord commits the companies to enforcing anti-scam policies in a "timely manner," sharing threat intelligence with industry peers and law enforcement, adding fraud detection tools (including AI-powered tools), introducing stronger verification requirements for financial transactions, and providing clear reporting channels for users who encounter scams.[475] The signatories also acknowledge the cross-platform nature of modern scams—where criminals typically initiate contact on social media, build trust on dating apps, and direct victims to external payment channels—and commit to coordinating a cross-platform response.[476]

Notably, these four groups—along with others—are built around some form of data or intelligence sharing, whether through real-time API integrations, signal clearinghouses, direct platform-to-bank partnerships, or working groups sharing threat typologies. The recognition that no single sector can see the full picture of how criminal networks operate has made cross-sector data sharing the foundational strategy.

B. <u>Examples of Initiatives from the Trump Administration</u>

Since the start of 2026, the Trump Administration has pursued one of the most ambitious federal anti-fraud agendas in recent history, issuing major EOs, announcing a new DOJ enforcement division, and establishing a White House-led task force. Together, these actions represent a significant restructuring of how the federal government coordinates its response to cybercrime, online scams, and fraudulent exploitation of American taxpayers. In fact, according to DOJ Criminal Division Associate Counsel Richard Goldberg, "[the Administration] and its agency partners are more focused than ever on dismantling TCOs responsible for causing the

---

[469] Meta, Partners with UK Banks, *supra* note 32; ASPEN INST., SCALING SCAM PREVENTION, *supra* note 33.
[470] Meta, Partners with UK Banks, *supra* note 32.
[471] Briefings with Committee Republican staff (notes on file with the Committee).
[472] Briefings with Committee Republican staff (notes on file with the Committee).
[473] Fria Reyes, *Big Tech Creates "Accord Against Online Scams & Fraud"*, PRIVACY GUIDES (Mar. 22, 2026), https://www.privacyguides.org/news/2026/03/22/big-tech-creates-accord-against-online-scams-fraud/.
[474] INDUSTRY ACCORD AGAINST ONLINE SCAMS & FRAUD (2026), *available at* https://services.google.com/fh/files/newsletters/industryaccord.pdf.
[475] *Id.*
[476] *Id.*

unprecedent[ed] billions of dollars in losses to American victims."[477] This Administration's DOJ, in particular, has reportedly "substantially increased its fight against cryptocurrency investment fraud schemes, the scam compounds that perpetrate such crimes, and the networks that launder their fraud proceeds."[478] Agencies are also increasingly collaborating with foreign law enforcement to combat the criminals perpetrating fraud and scams.[479]

1. *Executive Orders and Other Regulatory Actions*

Since taking office, President Trump has issued several EOs and taken other actions focused on addressing fraud and scams.

- On March 20, 2025, President Trump signed an EO titled "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos."[480] The EO stated that "[r]emoving unnecessary barriers to federal employees accessing Government data and promoting inter-agency data sharing are important steps toward eliminating bureaucratic duplication and inefficiency while enhancing the Government's ability to detect overpayments and fraud."[481] This early order focused on the importance of information sharing across the government, which is critical to anti-fraud and anti-scam efforts.[482]

- On March 25, 2025, President Trump signed an EO titled "Protecting America's Bank Account Against Fraud, Waste, and Abuse."[483] This EO focused on "enabling the Department of the Treasury to more easily conduct improper payment and fraud prevention screening prior to disbursing funds on behalf of agencies." [484] This early order focused on the internal integrity of federal financial systems, setting the stage for subsequent broader anti-fraud actions.[485]

- On March 25, 2025, President Trump signed an EO titled, "Modernizing Payments to and From America's Bank Account," which directed the Treasury Department to discontinue the use of paper checks for federal disbursements due to the heightened risk of check fraud.[486] In response, on May 30, 2025, the Treasury Department released a Request for Information (RFI), which stated that "[p]aper checks are increasingly the front door for fraud," and therefore requested comments on recommendations "to advance a public awareness campaign that will help consumers,

---

477 *J. Econ. Comm.*, *supra* note 11 (statement of Richard Goldberg, Associate Counsel, Criminal Division, U.S. Dep't of Just.).
478 *Id.*
479 *Id.*
480 Exec. Order No. 14,243, *supra* note 34.
481 *Id.*
482 Exec. Order No. 14,249, *supra* note 34.
483 *Id.*
484 *Id.*
485 *Id.*
486 Exec. Order No. 14,247, 90 Fed. Reg. 14,001 (2025), *available at* https://www.federalregister.gov/documents/2025/03/28/2025-05522/modernizing-payments-to-and-from-americas-bank-account.

including unbanked and underbanked populations, transition to digital payments[.]"[487]

Beginning September 30, 2025, the federal government stopped issuing paper checks for most federal payments subject to various exemptions.[488] According to the Trump Administration, this will "help reduce fraud and theft" and "remove delays that prevent hardworking Americans from receiving their vital payments."[489] For example, Treasury checks are 16 times more likely to be reported lost or stolen, returned undeliverable, or altered than an EFT.[490] In addition to moving away from physical Treasury checks, the Treasury Department has sought enhancements to its Treasury Check Verification System (TCVS).[491] The TCVS is designed to verify the validity of government checks and their payee information, but sophisticated criminals have developed tools to counterfeit checks that pass TCVS verification, and operational difficulties have limited the ability of financial institutions to easily connect.[492] To address these challenges, ABA collaborated with the Treasury Department to develop its own interface to permit easier connectivity to the Treasury Department's TCVS while ensuring robust protection of Americans' personally identifiable information.[493] More than 600 banks have used the ABA interface to validate more than 11,000 checks.[494]

- In June 2025, the Board of Governors of the Federal Reserve System (Federal Reserve), Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency (jointly, the Agencies) jointly released a RFI to address payments and check fraud.[495] The Agencies requested potential actions "to help consumers, businesses, and financial institutions mitigate check, automated clearing house (ACH), wire, and instant financial fraud."[496] Further, the Agencies admit that "no single agency or private-sector entity can address financial fraud on its own."[497] The Agencies sought private sector input on several questions, including external

---

487 Request for Information, U.S. Dep't of the Treasury, 90 Fed. Reg. 23,108 (May 30, 2025), *available at* https://www.federalregister.gov/documents/2025/05/30/2025-09766/request-for-information-related-to-the-executive-order-modernizing-payments-to-and-from-americas.
488 Press Release, U.S. Dep't of the Treasury, Treasury Announces Federal Government Will Phase Out Paper Checks on September 30th (Aug. 14, 2025), https://home.treasury.gov/news/press-releases/sb0223.
489 *Id.*
490 News Release, Bureau of the Fiscal Serv., U.S. Dep't of the Treasury, Paper Checks Are Going Away – Here's What You Need to Know (Aug. 14, 2025), https://fiscal.treasury.gov/news/paper-checks-going-away.html.
491 News Release, Bureau of the Fiscal Serv., U.S. Dep't of the Treasury, Treasury Check Verification System (TCVS) Payee Name Validation Reminder (June 4, 2025), https://www.frbservices.org/news/communications/060925-treasury-check-verification-system.
492 *Fraud in Focus*, *supra* note 42 (testimony of Paul Benda, Am. Bankers Ass'n).
493 *Id.*
494 *Id.*
495 Request for Information on Potential Actions to Address Payments Fraud, U.S. Dep't of the Treasury, Bd. of Governors of the Fed. Rsrv. Sys., Fed. Deposit Insurance Corp., 90 Fed. Reg. 26,293 (June 20, 2025) (request for information and comment), https://www.federalregister.gov/documents/2025/06/20/2025-11280/request-for-information-on-potential-actions-to-address-payments-fraud.
496 *Id.*
497 *Id.*

collaboration, consumer education, data collection and information sharing, and tools and services provided by Reserve Banks.[498]

- On August 4, 2025, FinCEN issued notice FIN-2025-NTC1, urging financial institutions to be vigilant in identifying and reporting suspicious activity involving convertible virtual currency kiosks, also commonly referred to as crypto ATMs.[499] The notice highlighted that criminals engaged in fraud schemes frequently direct victims to use crypto ATMs to send payments under false pretenses.[500] Lastly, FinCEN explained how crypto ATMs work, and how some crypto ATM operators provide financial institutions with false information to appear compliant with FinCEN requirements.[501]

- On September 8, 2025, FinCEN issued FIN-2025-NTC2 to help financial institutions detect and disrupt financially motivated sextortion.[502] FinCEN noted that this typology has become increasingly common and has devastating effects on victims and their families.[503] FinCEN provided information on how sextortion works, payment methods associated with the sextortion scheme, and how scammers use money mules.[504]

- On October 14, 2025, FinCEN issued a final rule in which it severed Cambodia-based Huione Group from the U.S. financial system after finding the group represented a "financial institution of primary money laundering concern."[505] Huione Group not only worked closely with scam centers in Southeast Asia, but also with cyber hackers backed by North Korea.[506] FinCEN's rule barred covered financial institutions "from opening or maintaining correspondent accounts for or on behalf of Huione Group" and also required the institutions to apply due diligence on use of foreign correspondent accounts.[507] Notably, shortly thereafter, in December 2025, the National Bank of Cambodia—the country's central bank—revoked Huione Group's

---

498 *Id.*
499 FIN. CRIMES ENF'T NETWORK, FIN-2025-NTC1, *supra* note 332.
500 *Id.*
501 *Id.*
502 FIN. CRIMES ENF'T NETWORK, FIN-2025-NTC2, FINCEN NOTICE ON FINANCIALLY MOTIVATED SEXTORTION, (2025), *available at* https://www.fincen.gov/system/files/2025-09/FinCEN-Notice-FMS-508C.pdf.
503 *Id.*
504 *Id.*
505 News Release, Fin. Crimes Enf't Network, FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System (Oct. 14, 2025), https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-severing-huione-group-us-financial-system.
506 *Id.*
507 *See* U.S. Dep't of the Treasury, Imposition of Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern, 90 Fed. Reg. 48,295 (Oct. 16, 2025) (final rule). The rule became effective on November 17, 2025. *Id.*

operating license.[508] In June 2026, FinCEN proposed to extend its rule to cover H-Pay Service PLC and any successor entity.[509]

- Also on October 14, 2025, the Administration took a series of coordinated actions against the Prince Group, a TCO that operated scam centers in Cambodia. According to the Treasury Department, "Prince Group TCO [was] a dominant player in Cambodia's scam economy and has controlled illicit financial flows of billions of dollars."[510] OFAC imposed sanctions on 146 entities and individuals associated with the Prince Group.[511] The FBI also indicted the leader of the Prince Group, Chen Zhi.[512] Through the coordinated actions, the FBI was able to recover approximately $15 billion worth of bitcoin that were proceeds of the Prince Group's crimes, representing "one of the largest financial fraud takedowns in history."[513] In June 2026, Treasury expanded its efforts to sanction another nine individuals and 26 entities associated with the Prince Group.[514]

- On October 28, 2025, the FCC adopted a Second Further Notice of Proposed Rulemaking (FNPRM) proposing requirements for voice providers to give consumers accurate caller identity information, ensuring they no longer have to guess whether a call is one the consumer wishes to answer.[515] This also was designed to combat illegal calls originating from overseas.[516] The FNPRM also sought comment on "how providers can comply with the requirement to ensure broadband labels are prominently displayed, publicly available, and easily accessible to consumers with disabilities when there is no requirement that providers read the label to consumers over the phone."[517]

  This effort built on the FCC's actions from August 2025, in which the Commission removed 1,388 non-compliant voice service providers from the database for false, misleading, or outdated filings, and new rules effective February 2026 impose $10,000 per-violation fines for inaccurate Robocall Mitigation Database (RMD)

---

[508] Sam Ellefson, *Cambodian payment processor freezes customer funds before regulators shut it down*, INT'L CONSORTIUM OF INVESTIGATIVE JOURNALISTS (Dec. 9, 2025), https://www.icij.org/investigations/coin-laundry/cambodian-payment-processor-freezes-customer-funds-before-regulators-shut-it-down/.
[509] Press Release, U.S. Dep't of Treasury, Treasury Further Dismantles Overseas Scam Operations Targeting Americans (June 23, 2026), https://home.treasury.gov/news/press-releases/sb0538 [hereinafter Treasury Further Dismantles Overseas Scam Operations].
[510] U.S. Dep't of the Treasury, U.S. and U.K. Take Largest Action Ever, *supra* note 21.
[511] *Id.*
[512] Press Release, U.S. Dep't of Just., Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes (Oct. 14, 2025), https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged.
[513] *Id.*
[514] Treasury Further Dismantles Overseas Scam Operations, *supra* note 509.
[515] FED. COMMC'N COMM'N, FCC-25-74, EMPOWERING BROADBAND CONSUMERS THROUGH TRANSPARENCY (2025), *available at* https://docs.fcc.gov/public/attachments/FCC-25-74A1.pdf.
[516] *Id.*
[517] Announcement, Fed. Commc'ns Comm'n, FCC Seeks Comments on Changes to Broadband labels for Consumers, https://www.fcc.gov/consumer-governmental-affairs/fcc-seeks-comments-changes-broadband-labels-consumers (last visited June 4, 2026).

filings.[518] To strengthen harmonization, the traceback rules within the STIR/SHAKEN framework also allow the FCC to conduct oversight across multiple private-sector filings to trace back suspected illegal calls to the source.[519]

In addition to STIR/SHAKEN, the Pallone-Thune TRACED Act also established rulemaking for Know Your Customer (KYC) and Know Your Upstream Provider (KYUP) initiatives which seeks to establish due diligence standards on telecommunications providers.[520] While the rules have yet to be implemented, both rulemakings seek to eliminate bad actors, close network gaps, improve traceability, and enforce telecommunications ecosystem accountability.[521] The KYC rulemaking seeks to accomplish these goals by incentivizing providers to be thorough in ensuring the initial communication sent out by bad actors are blocked at the very beginning of the call path.[522] On the other hand, KYUP rulemaking seeks to obtain these objectives by forcing downstream telecommunications companies to audit and verify the legitimacy of intermediate carriers.[523]

- On January 8, 2026, the White House announced the creation of the DOJ's Division for National Fraud Enforcement (NFED), a new DOJ division intended to centralize and elevate the federal government's approach to fraud enforcement.[524] The NFED is led by an Assistant Attorney General responsible for (1) leading multi-district and multi-agency fraud investigations; (2) shaping national enforcement priorities across DOJ components; (3) advising DOJ leadership on significant fraud matters affecting federal programs, federally funded benefits, businesses, nonprofits, and private citizens; and (4) working with other departments to identify, disrupt, and dismantle organized and sophisticated fraud schemes that cross jurisdictions.[525] On March 24, 2026, Colin McDonald was confirmed as the as the Division's first Assistant Attorney General.[526] The NFED represents a structural consolidation of fraud-enforcement resources that had previously been fragmented across multiple DOJ components.

- On March 5, 2026, the FCC released a draft Notice of Proposed Rulemaking (NPRM) proposing changes to its telephone numbering policies,[527] which was formally

---

[518] Briefings with Committee Republican staff (notes on file with the Committee).
[519] FED COMMC'NS COMM'N, ENHANCING STIR-SHAKEN TO COMBAT ILLEGAL ROBOCALLS 3 (2026).
[520] *Id.* at 6.
[521] *Id.*
[522] *Id.*
[523] *Id.*
[524] Fact Sheet, White House, President Donald J. Trump Establishes New Department of Justice Division for National Fraud Enforcement (Jan. 8, 2026), https://www.whitehouse.gov/fact-sheets/2026/01/fact-sheet-president-donald-j-trump-establishes-new-department-of-justice-division-for-national-fraud-enforcement/.
[525] *Id.*
[526] Jaclyn Diaz, *Senate Confirms Trump's Pick for New Role of Fraud Enforcement at Justice Department*, NPR (Mar. 24, 2026), https://www.npr.org/2026/03/24/g-s1-114956/trump-fraud-enforcement-justice-role.
[527] FED. COMMC'N COMM'N, FCC-CIR2603-01, IMPROVING CUSTOMER SERVICE AND CONSUMER PROTECTION IMPROVING CUSTOMER SERVICE AND PROTECTING CONSUMERS THROUGH ONSHORING; ADVANCED METHODS TO TARGET AND ELIMINATE UNLAWFUL ROBOCALLS; RULES AND REGULATIONS IMPLEMENTING THE TELEPHONE CONSUMER PROTECTION ACT OF 1991 (2026), *available at* https://docs.fcc.gov/public/attachments/DOC-419247A1.pdf.

adopted at the FCC's March 26, 2026, open meeting.[528] The changes are designed to make it harder for bad actors to obtain and exploit numbering resources to make robocalls.[529] The NPRM proposes to extend robocall-related certification obligations to all voice service providers that receive numbering resources directly from the North American Numbering Plan Administrator.[530] Further, it would require covered providers and resellers to certify that they will not knowingly facilitate illegal robocalls, illegal spoofing, or fraud.[531] The NPRM also seeks comment on number "cycling," the practice of rotating through large quantities of telephone numbers, often on a single-use basis to evade robocall detection.[532]

- The most comprehensive of the Administration's fraud-related executive actions came on March 6, 2026, when President Trump signed EO 14390, "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens."[533] The order reflects growing federal concern about large-scale cyber fraud operations run by TCOs, and targets schemes, including ransomware attacks, phishing campaigns, impersonation scams, sextortion, and other forms of cyber-enabled financial fraud.[534]

  The EO importantly directs the Attorney General, and other federal partners, to examine how "operational, technical, diplomatic, and regulatory frameworks . . . can be improved to best combat TCOs engaged in cyber-enabled crime and similar predatory schemes against Americans[.]"[535] Within 120 days, relevant agencies are required to deliver to the President an action plan identifying the specific TCOs responsible for scam centers and cybercrime, and proposing concrete solutions to prevent, disrupt, investigate, and dismantle their operations.[536] Critically, the EO also directs "the creation of an operational cell within the National Coordination Center (NCC)," to help coordinate "[f]ederal efforts to detect, disrupt, dismantle, and deter – including by involving the private sector as appropriate—cyber-enabled criminal activity conducted by foreign TCOs and associated networks that target United States persons, businesses, critical infrastructure, or public services."[537] The order included provisions directed at establishing mechanisms to seek forfeiture of stolen funds and return them to victims "to the maximum extent possible"—an acknowledgment that financial recovery for fraud victims has historically been inadequate.[538]

---

[528] FED. COMMC'N COMM'N, FCC PROPOSES CALL CENTER ONSHORING, ENGLISH PROFICIENCY REQUIREMENTS (2026), *available at* https://docs.fcc.gov/public/attachments/DOC-420129A1.pdf.
[529] *Id.*
[530] *Id.*
[531] *Id.*
[532] *Id.*
[533] Exec. Order No. 14,390, 91 Fed. Reg. 12,051 (2026), https://www.federalregister.gov/documents/2026/03/11/2026-04826/combating-cybercrime-fraud-and-predatory-schemes-against-american-citizens.
[534] *Id.*
[535] *Id.* Other federal partners involved in this effort include the Secretary of State, the Secretary of the Treasury, the Secretary of War, and the Secretary of Homeland Security. The Office of the National Cyber Director and the Assistant to the President and Homeland Security Advisor will also participate in coordination efforts. *Id.*
[536] *Id.*
[537] *Id.*
[538] *Id.*

Beyond these efforts, some agencies are investing in technological capabilities to be able to identify and stop fraud and scams. For example, the Federal Reserve is developing tools through which it can ensure that payments are being sent to the individual and company they are purported to reach.[539] Such technology could be made available to member institutions and help to prevent instances in which a scammer purports to be someone else.[540]

2. *Scam Center Strike Force*

In November 2025, the Administration announced the launch of the Scam Center Strike Force, which combined the "power, reach, and resources of the U.S. Attorney's Office with the DOJ's Criminal Division, the FBI, and the U.S. Secret Service to secure America against Southeast Asian cryptocurrency-related fraud and scams."[541] At its launch, U.S. Attorney Jeanine Pirro laid out the Strike Force's core mission: identify the entities behind digital asset scams, charge their leaders, seize stolen funds, and shut down any infrastructure subject to U.S. jurisdiction.[542]

The Strike Force extends beyond its core members. It also closely collaborates with the Department of State, OFAC, and the Department of Commerce, the Internal Revenue Service, the U.S. Postal Inspection Service, and the Drug Enforcement Agency.[543] The Strike Force is also using public-private partnerships to ensure that U.S. infrastructure is not abused to perpetrate these crimes against Americans.[544]

The Strike Force moved quickly after its November 2025 launch. Within weeks, it seized fake digital asset investment domains being used by the Tai Chang scam compound—also known as Casino Kosai—in Burma.[545] According to the Strike Force, the seized domains "directed users to download mobile applications—linked to the scam—from Google Play and the Apple App Store."[546] The FBI allegedly worked closely with tech platforms, including Google, Apple, and Meta, to remove the fraudulent domains from their platforms.[547]

In April 2026, the Strike Force announced a sweeping wave of coordinated actions. Authorities unsealed criminal complaints against two Chinese nationals—Huang Xingshan and Jiang Wen Jie—who served as managers at the Shunda compound in Min Let Pan, Burma.[548] Huang was a manager who reportedly used violence against trafficked workers, while Jiang

---

539 Briefing with Committee Republican staff (notes on file with the Committee).
540 Briefing with Committee Republican staff (notes on file with the Committee).
541 *Scam Center Strike Force*, U.S. ATT'Y OFF. FOR THE DIST. OF COLUMBIA, https://www.justice.gov/usao-dc/scam-center-strike-force (last visited June 25, 2026).
542 *Id.*
543 *Id.*
544 *Id.*
545 News Release, Fed. Bureau of Investigation, FBI San Diego Investigation Leads to Scam Center Strike Force Seizure of Fake Cryptocurrency Investment Domain Used by Tai Chang Scam Compound in Burma (Dec. 2, 2025), https://www.fbi.gov/contact-us/field-offices/sandiego/news/fbi-san-diego-investigation-leads-to-scam-center-strike-force-seizure-of-fake-cryptocurrency-investment-domain-used-by-tai-chang-scam-compound-in-burma.
546 *Id.*
547 *Id.*
548 Press Release, U.S. Att'y Office for the Dist. of Columbia, Scam Center Strike Force Takes Major Actions Against Southeast Asian Scam Centers Targeting Americans (Apr. 23, 2026), https://www.justice.gov/usao-dc/pr/scam-center-strike-force-takes-major-actions-against-southeast-asian-scam-centers.

supervised their efforts to defraud Americans.[549] After the Shunda compound was seized, the two attempted to replicate their scheme at a compound in Cambodia but were arrested by Thai law enforcement for immigration violations while attempting to return to Burma.[550] As part of these coordinated actions, the Strike Force conducted a first-of-its-kind seizure of a Telegram channel with more than 6,000 followers that had been used to recruit individuals to travel to Cambodia under false promises of high-paying employment, where they were then held against their will and forced to commit fraud.[551] Alongside that, the Strike Force seized 503 fraudulent web domains used to execute investment scams against American victims.[552]

The April 2026 actions also extended into financial sanctions and diplomatic pressure. The Treasury Department's OFAC designated Cambodian Senator Kok An, his business empire, and 28 other individuals and entities—including casinos, front companies, and a Cambodian bank—for their roles in housing and facilitating human trafficking and cyber-enabled fraud.[553] The State Department simultaneously announced a reward of up to $10 million for information leading to the seizure of proceeds related to the Tai Chang scam center in Burma.[554]

The Strike Force continues to focus on "investigating the worst scam compounds located in Southeast Asia" and "identifying and pursuing key leaders—including Chinese organized crime affiliates operating in Cambodia, Laos, and Burma—to bring them to justice."[555] Thus far, beyond indictments and domain seizures, the Strike Force has also seen successful financial results. Freezes and seizures of digital assets from Southeast Asian crime networks alleged to be tied to money laundering from digital asset scams exceeds $725 million.[556]

The Strike Center is also working to collaborate with other public and private sectors. In May 2026, the Strike Center led a "a first-of-its-kind event" bringing together public and private stakeholders to "tackle cyber-enabled and cryptocurrency fraud targeting Americans."[557] Dubbed "Disruption Week," the participants—which included U.S. government law enforcement entities, foreign government representatives, Apple, Coinbase, Google, Meta, Microsoft, SpaceX, TRM

---

[549] Criminal Complaint at 31-32, United States v. Huang Xingshan, Case 1:26-mj-00018-MAU (D.D.C. Apr. 23, 2026), https://www.justice.gov/usao-dc/media/1437601/dl?inline; Criminal Complaint at 32, United States v. Jiang Wen Jie, Case 1:26-mj-00017-MAU, Complaint (D.D.C. Apr. 23, 2026), https://www.justice.gov/usao-dc/media/1437611/dl?inline.

[550] Press Release, U.S. Att'y Office for the Dist. of Columbia, *supra* note 548; Criminal Complaint at 31-32, United States v. Huang Xingshan, *supra* note 549; Criminal Complaint at 32, United States v. Jiang Wen Jie, *supra* note 549.

[551] Press Release, U.S. Att'y Office for the Dist. of Columbia, *supra* note 548; Application for a Warrant to Seize Property Subject to Forfeiture, In re Seizure of One Telegram Channel, Case No. 26-sz-32 (D.D.C. Apr. 22, 2026), https://www.justice.gov/usao-dc/media/1437596/dl?inline.

[552] Press Release, U.S. Att'y Office for the Dist. of Columbia, *supra* note 548.

[553] Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Cambodian Senator Kok An and Scam Center Network Defrauding Americans (Apr. 23, 2026), https://home.treasury.gov/news/press-releases/sb0469.

[554] Press Statement, U.S. Dep't of State, Imposing Sanctions on Online Scam Centers in Southeast Asia (Apr. 23, 2026), https://www.state.gov/releases/office-of-the-spokesperson/2026/04/imposing-sanctions-on-online-scam-centers-in-southeast-asia-2.

[555] *Scam Center Strike Force*, *supra* note 541.

[556] *Id.*

[557] Press Release, U.S. Dep't of Just., Scam Center Strike Force Announces Results of U.S. & Private Industry "Disruption Week" (June 3, 2026), https://www.justice.gov/opa/pr/scam-center-strike-force-announces-results-us-private-industry-disruption-week.

Labs, and others—worked together to "interrupt millions of social media, email, and internet access accounts" used by criminals operating in scam centers, and voluntary froze "over $3.8 million in cryptocurrency involved in laundering of funds stolen from Americans."[558] The participants also reportedly "voluntarily exchanged information" on how criminals operate and agreed to continue cooperating to "enable future disruptions of scams occurring on U.S. networks."[559]

3. *Other Government Interagency Groups & Task Forces*

Like the private sector, the public sector has also developed inter-agency and intra-agency partnerships to better share information on fraud and scams issues. In many cases, these are informal arrangements that are largely driven by trusted relationships among officials over a long period of time.[560] However, others are more established processes, including:

- In addition to the Scam Center Strike Force, the DOJ also leads an interagency initiative targeting financial crimes against older Americans—the DOJ Elder Fraud Strike Force. Originally launched in 2019, the Strike Force was significantly expanded in 2022, growing from 6 to 20 participating U.S. Attorney's Offices — now covering all offices in California, Arizona, Texas, Florida, Georgia, Maryland, and New York. The Strike Force brings together U.S. Attorneys with the FBI, U.S. Postal Inspection Service, and Homeland Security Investigations. Its cases span mass-marketing scams, lottery and prize fraud, tech support impersonation, grandparent scams, and government impersonation. In the period from July 2023 to June 2024 (the most recent annual reporting period), the DOJ pursued over 300 enforcement actions against more than 700 defendants charged with stealing nearly $700 million from approximately 225,000 victims. During the same period, the DOJ provided services and assistance to over 230,000 older victims and returned more than $31 million to them. Local iterations of the FBI-led Elder Justice Task Force (EJTF) operate in cities including San Diego and elsewhere, partnering local law enforcement and prosecutors with federal agents to dismantle locally active fraud rings — many of which originate at overseas call centers and use local money launderers to move funds offshore.

- The SEC has created two task forces related to fraud and scams. By 2023, SEC staff identified a need for increased coordination and collaboration to combat these crimes given asymmetric capabilities across entities.[561] As a result, the SEC created the Interagency Securities Council (ISC).[562] The ISC "invites federal, state, and local regulatory and law enforcement professionals to meet quarterly to discuss the latest in scams, trends, frauds, and mitigation strategies."[563] The ISC intends "to strengthen the cohesion between federal, state, and local agencies, enhance opportunities to

---

558 *Id.*
559 *Id.*
560 Briefings with Committee Republican Staff (notes on file with the Committee).
561 Briefings with Committee Republican Staff (notes on file with the Committee).
562 Briefings with Committee Republican Staff (notes on file with the Committee).
563 Press Release, Sec. & Exch. Comm'n, SEC Launches Interagency Securities Council to Coordinate Enforcement Efforts Across Federal, State, and Local Agencies (July 19, 2024), https://www.sec.gov/newsroom/press-releases/2024-86.

collaborate on cases to protect investors, provide insight and guidance across the ecosystem to those who may not frequently operate in this space, and create a forum for unified efforts in combating financial fraud."[564] Importantly, representatives from over 100 local, state, and federal agencies have joined the ISC.[565] The ISC's quarterly meetings and additional events seek to educate participants on trends and relevant technologies, including deepfakes and artificial intelligence.[566] The ISC is enhancing collaboration, streamlining operations, upskilling agency staff, and increasing awareness of common trends.

In September 2025, the SEC also established the Cross-Border Task Force to Combat Fraud (CBTF).[567] The CBTF was created to "strengthen and enhance the Division of Enforcement's efforts to identify and combat cross-border fraud harming investors."[568] More specifically, the CBTF is "focus[ed] initially on investigating potential U.S. federal securities law violations related to foreign-based companies, including potential market manipulation, such as "pump-and-dump" and "ramp-and-dump" schemes."[569] Further, the CBTF will also "focus enforcement efforts on gatekeepers, particularly auditors and underwriters, which help these companies access the U.S. capital markets. In addition, it will examine potential securities law violations related to companies from foreign jurisdictions, such as China, where governmental control and other factors pose unique investor risks."[570] As of February 2026, the CBTF had imposed fourteen trading suspensions of largely Asia-based issuers.[571] Although the SEC can only impose these suspensions for up to 10 business days,[572] the listing exchange can continue to suspend that entity based on its own authorities.[573]

- FINRA's newly launched Financial Intelligence Fusion Center (FIFC) offers a centralized information sharing portal to member broker-dealers for analyzing and disseminating threat intelligence.[574] The Center will leverage cross-jurisdictional partnerships across public and private entities for real-time information sharing. Given the pervasiveness and growing complexities of fraud and investment scams, information sharing tactics like the FIFC will be critical to preemptive investor protection.

- In response to digital assets having become a dominant typology,[575] in 2024, the FBI initiated "Operation Level Up," and deployed tools to "[disband] fraud and laundering syndicates, shut down scam call centers, [shutter] illicit marketplaces,

[564] *Id.*
[565] *Id.*
[566] Briefings with Committee Republican staff (notes on file with Committee).
[567] Press Release, Sec. & Exch. Comm'n, *supra* note 35.
[568] *Id.*
[569] *Id.*
[570] *Id.*
[571] Briefings with Committee Republican staff (notes on file with Committee).
[572] 15 U.S.C. § 78l(K); briefings with Committee Republican staff (notes on file with Committee).
[573] Briefings with Committee Republican staff (notes on file with Committee).
[574] BUSINESSWIRE, *supra* note 35.
[575] Briefings with Committee Republican staff (notes on file with Committee).

[dissolve] nefarious 'botnets,' and put hundreds of other actors behind bars."[576] Operation Level Up proactively "identified victims of cryptocurrency investment fraud and notified them of the scam."[577] The FBI notified 4,323 victims of digital asset investment fraud using IC3 data—and 76 percent of the victims were unaware that they were being scammed.[578] Importantly, these victims—and others—are referred to an FBI victim specialist for suicide intervention.[579] The Victim Services Division's "mission is connecting people—connecting victims to specialist teams and resources and then connecting investigative teams to victims and giving them a platform to speak."[580] It helps victims through the "aftermath of crime and the criminal justice process," and shares available resources.[581] The FBI has also collaborated with the DOJ and international law enforcement "to combat cyber-enabled financial crimes and transnational call center fraud."[582] Joint operations involving the FBI on these issues resulted in actionable leads and over 200 arrests.[583]

- FinCEN works to "safeguard the financial system from illicit activity, counter money laundering and the financing of terrorism, and promote national security through strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence."[584] FinCEN collects financial intelligence, including Suspicious Activity Reports (SARs), "which select financial institutions are mandated to file if they suspect certain fraud, scams, or other potential illicit activity."[585] FinCEN employes several authorities to combat fraud and scams. Most notably, it runs a Rapid Response Program (RRP), which seeks to recover stolen funds from cyber-enabled scams.[586] According to FinCEN staff, part of the program's goal is to more rapidly share information with Financial Intelligence Units (FIUs) around the world.[587] Each of FinCEN's international counterparts have their own unique, respective jurisdictions.[588] Although there are not formal memoranda of understanding between FinCEN and these FIUs, each FIU is encouraged to use their own respective networks to address issues.[589] A case led by the RRP typically begins with a complaint from either a victim or a financial institution, which is provided to law enforcement.[590] If law enforcement chooses to open the case, the law enforcement entity may bring FinCEN in where funds might be recoverable.[591]

[576] FBI 2025 INTERNET CRIME REPORT, *supra* note 25, at 3.
[577] *Id.* at 14.
[578] *Id.*
[579] *Id.*
[580] *Reaching Out to Assist Victims of Crime*, FED. BUREAU OF INVESTIGATION (May 20, 2024), https://www.fbi.gov/news/stories/reaching-out-to-assist-victims-of-crime.
[581] *Id.*
[582] FBI 2025 INTERNET CRIME REPORT, *supra* note 25, at 14.
[583] *Id.*
[584] *About FinCEN*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/about-fincen (last visited Mar. 25, 2026).
[585] U.S. GOV'T ACCOUNTABILITY OFF., IF13094, FINANCIAL FRAUD AND SCAMS: THE ROLES OF FEDERAL LAW ENFORCEMENT AND FINANCIAL REGULATORS (2025).
[586] Briefings with Committee Republican staff (notes on file with Committee).
[587] Briefings with Committee Republican staff (notes on file with Committee).
[588] Briefings with Committee Republican staff (notes on file with Committee).
[589] Briefings with Committee Republican staff (notes on file with Committee).
[590] Briefings with Committee Republican staff (notes on file with Committee).
[591] Briefings with Committee Republican staff (notes on file with Committee).

Following receipt of referral, FinCEN will share information with the appropriate FIU.[592] In Fiscal Year 2025, the RRP helped 392 victims, which included both individuals and businesses, but supported the investigations of over 800 transactions.[593] Notably, one stakeholder flagged limitations to the RRP related to digital asset scams—because victims may not become aware of the scam right away, the RRP is more limited in effectiveness.[594] By contrast, the stakeholder described RRP as "most impactful" in business email compromise.[595]

- The Treasury Department also maintains the Financial Literacy and Education Commission (FLEC), which is tasked with creating a national strategy on financial education.[596] The Secretary of the Treasury chairs FLEC, with 22 other federal agencies participating.[597] "FLEC provides a forum for its [participants] to coordinate their efforts to advance financial literacy and education. FLEC represented agencies develop consumer-friendly, trustworthy, and consistent educational materials and tools, and conduct outreach efforts to help consumers make informed and sound decisions that enhance their financial well-being."[598]

  As part of its mandate, FLEC hosts public meetings, each focused on different topics. The September 2025 meeting focused largely on the threat presented by fraud and scams, with panels addressing (1) national trends in financial fraud and (2) implementation of Executive Order 14247 on Modernizing Federal Payments.[599] At least one stakeholder noted that FLEC could present a useful convening mechanism to share information across the federal government, given the volume of members.[600] However, other stakeholders acknowledged that FLEC has not been as successful or productive as intended.[601]

---

[592] Briefings with Committee Republican staff (notes on file with Committee).
[593] Briefings with Committee Republican staff (notes on file with Committee).
[594] Briefings with Committee Republican staff (notes on file with Committee).
[595] Briefings with Committee Republican staff (notes on file with Committee).
[596] *Financial Literacy and Education Commission*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/consumer-policy/financial-literacy-and-education-commission.
[597] *Id.* The other participants include: Commodity Futures Trading Commission, Department of Agriculture, Department of Defense, Department of Education, Department of Health and Human Services, Department of Housing and Urban Development, Department of Interior, Department of Labor, Department of Veterans Affairs, Federal Deposit Insurance Corporation, Federal Emergency Management Agency, Federal Housing Finance Agency, Federal Reserve Board, Federal Trade Commission, General Services Administration, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Personnel Management, Small Business Administration, Securities and Exchange Commission, Social Security Administration, and the White House Domestic Policy Council. *Id.*
[598] Request for Information Related to the Financial Literacy and Education Commission (FLEC) Update to the U.S. National Strategy for Financial Literacy, U.S. Dep't of the Treasury, 91 Fed. Reg. 5,036 (Feb. 3, 2026).
[599] *Agenda*, *FLEC Public Meeting*, U.S. DEP'T OF THE TREASURY (Sep. 24, 2025), https://home.treasury.gov/system/files/136/September-2025-FLEC-Public-Meeting-Agenda.pdf.
[600] Briefings with Committee Republican staff (notes on file with Committee).
[601] Briefings with Committee Republican staff (notes on file with Committee).

C. Notable State & Local Efforts

While federal agencies attract the most public attention in the fight against fraud and scams, state and local governments are an indispensable—and in some cases faster-moving—layer of anti-fraud infrastructure. State attorneys general, local law enforcement agencies, and specialized intelligence centers collectively represent a vast front line of defense, reaching communities and combating fraud typologies that federal agencies cannot always address at the scale required. With consumers losing billions in fraud every year, the pressure on state and local actors to fill gaps in the response has never been greater.

State Attorneys General and State Regulators. State attorneys general are among the most visible and consequential actors in the state-level anti-fraud landscape. Their authority spans consumer protection, securities law, and general civil and criminal enforcement, giving them a broad toolkit for pursuing fraud across industries.[602] Although offices are taking steps independently to address these issues, like their federal counterparts, they are also seeking broad coalitions and coordinated actions, which allow smaller states to pool resources and legal capacity. It also has the benefit of sending a stronger deterrent signal to bad actors than any single state action could. As one example of these efforts, in June 2025, a bipartisan coalition of 42 state and territory attorneys general sent a letter to Meta urging the company to take immediate action against fraudulent investment advertisements on Facebook and WhatsApp.[603] The letter, organized through the National Association of Attorneys General (NAAG), noted that deceptive ads lure users into fraudulent investment groups through the impersonation of trusted individuals, such as prominent financial figures, resulting in significant losses.[604] Such scams "can be initiated and disseminated on your platforms with alarming ease, targeting our most vulnerable population."[605] State regulators are also working to address the prevalence of fraud and scams. They do this by issuing alerts, shutting down scam websites, partnering with blockchain analytics firms to trace and recover stolen digital assets, and tracking the use of AI-powered scam tools.

Specialized Financial Crime Centers. Beyond attorneys general and regulators, some states have developed specialized capacity for financial crimes investigation. Most notable is the Texas Financial Crimes Intelligence Center (Texas FCIC or the Center). Operating as a first-of-its-kind fusion center, Texas FCIC was created in 2021, officially opening in January 2022.[606] The Center was created in part because many fraud and scams are carried out by organized criminal enterprises, and a statewide fusion center, with both law enforcement and analytical capacity, is necessary to track these networks and coordinate a response that spans county and municipal boundaries.[607] "The [FCIC] is staffed by law enforcement officers and analysts with

---

[602] *See Attorney General 101*, LEADERSHIP CENTER FOR ATTORNEY GENERAL STUDIES, https://agstudies.org/attorney-general-101/.
[603] Press Release, Nat'l Ass'n of Attys Gen., 42 State and Territory Attorneys General Urge Meta to Take Action Against Investment Scam Ads (June 11, 2025), https://www.naag.org/press-releases/42-state-and-territory-attorneys-general-urge-meta-to-take-action-against-investment-scam-ads/.
[604] *Id.*
[605] *Id.*
[606] Jacob Putman, *What is the Financial Crimes Intelligence Center?*, TX. DIST. & CTY ATTYS ASS'N (May-June 2023), https://www.tdcaa.com/journal/what-is-the-financial-crimes-intelligence-center/.
[607] *About The FCIC*, TX. FIN. CRIMES INTEL. CTR., https://fcic.texas.gov/ (last visited Mar. 25, 2026).

extensive experience in financial and organized crime investigations."[608] It operates a secure intelligence portal through which law enforcement agencies across Texas can make direct submissions to the FCIC's database, enabling rapid aggregation of data from across the state.[609]

The Texas FCIC collaborates with local, state, and federal law enforcement agencies, as well as private industry stakeholders, to address, prevent, and mitigate financial crimes.[610] For example, the FCIC engages closely with U.S. Customs and Border Protection (CBP) and the U.S. Department of Homeland Security's Homeland Security Investigations (HSI) as well as the FBI.[611] In fact, the Texas FCIC has trained CBP and HSI on how to identify skimmers,[612] which are devices placed on various types of payment terminals (e.g. gas pumps, ATMs, and Point of Sale terminals in retail stores) to an individual's money or line of credit.[613] Additionally, the FCIC "provides training, technical, analytical, and investigative assistance to law enforcement agencies across Texas and the United States."[614]

In just the few short years of its existence, Texas FCIC has been incredibly successful in identifying, disrupting, and prosecuting criminal actors that target Americans. Recently, the Texas FCIC "announced the arrest of two individuals connected to a multi-state gift card fraud scheme spanning Illinois, Missouri, Oklahoma, and Texas."[615] In August 2025, Texas FCIC assisted in the indictments of 15 individuals relating to a $2.9 million money laundering scheme.[616] The investigation—done jointly by Texas FCIC investigators, U.S. Secret Service's Baltimore and Houston offices, the U.S. Department of Health and Human Services' Office of Inspector General, and the Houston Police Department—also identified several wire fraud schemes, romance scams, fake investment scams, and fraudulent vacant land sales.[617]

---

[608] *Id.*
[609] Putman, *supra* note 37.
[610] *About The FCIC*, TX. FIN. CRIMES INTEL. CTR., https://fcic.texas.gov/ (last visited Mar. 25, 2026); briefings with Committee Republican Staff (notes on file with Committee).
[611] Briefings with Committee Republican staff (notes on file with Committee).
[612] Briefings with Committee Republican staff (notes on file with Committee).
[613] *Resources for Consumers*, TX. FIN. CRIMES INTEL. CTR., https://fcic.texas.gov/consumer.html (last visited Mar. 25, 2026).
[614] *Resources for Law Enforcement*, TX. FIN. CRIMES INTEL. CTR., https://fcic.texas.gov/law-enforcement.html (last visited Mar. 25, 2026).
[615] News Release, Tx. Fin. Crimes Intel. Ctr., Texas Financial Crimes Intelligence Center Announces Arrests in Multi-State Gift Card (Mar. 25, 2026), *available at* https://www.tdlr.texas.gov/media/pressrelease/2026-03-25-financial-crimes-intelligence-center-announces-arrests.pdf.
[616] Lillie Davidson, *15 suspects charged in $2.9M money laundering scheme, Texas officials say*, FORT WORTH STAR-TELEGRAM (Aug. 6, 2025), https://www.msn.com/en-us/news/us/15-suspects-charged-in-29m-money-laundering-scheme-texas-officials-say/ar-AA1K1r8X.
[617] *Id.*

Exhibit M: List of Texas FCIC Successes[618]

FCIC IN THE NEWS

04/29/26: Gift card tampering ring busted in Hays County, millions in consumer loss prevented

12/29/25: Illegal immigrants allegedly ran multi-million-dollar gift card fraud scheme hitting stores daily across Texas

09/13/25: 10 charged after FCIC uncovers card skimming operation across Texas

08/06/25: 15 suspects charged in $2.9M money laundering scheme, Texas officials say

07/23/25: Three men arrested, accused in 'transnational' credit card skimmer operation

06/23/25: Governor Signs New Texas Law, Targets Growing Crime At The Pump

05/16/25: Romanian crew convicted in ATM skimming case

04/01/25: 5 members of 'sophisticated' organized crime ring from Romania arrested in Houston

03/12/25: Authorities thwart Dallas County credit card skimmer operation

02/13/25: Man convicted of credit card skimming in Smith County gets life sentence

02/13/25: Man pleads guilty in multi-state ATM skimming scheme

11/15/24: Theft ring stole nearly $300K worth of fuel from North Texas gas stations, warrant alleges

08/21/24: Man sentenced for diesel thefts across Texas, 3 others at large

06/27/24: Financial Crimes Intelligence Center in Tyler helps convict man of organized diesel fuel theft

06/26/24: Man Convicted For Diesel Fuel Thefts Across Texas Using Stolen Credit Card Info

06/20/24: Three arrested in Tarrant County in multi-state skimming scam

06/19/24: Three Romanian Nationals Arrested During ATM Skimmer Investigation in DFW Area

06/18/24: Three Romanian Nationals Arrested For Credit Card Skimming In DFW

06/18/24: Three arrested for using skimmers on Dallas-Fort Worth area ATMs

06/18/24: Dallas man gets 50 years for East Texas diesel theft operation

05/29/24: First defendant sentenced in federal ATM jackpotting case

05/22/24: Baytown ATM skimmer operation spreads to Houston; behind the scenes with detective

04/25/24: Baytown police bust credit card skimming operation, arrest duo with deep skimmers

08/02/23: Texas financial crime expert speaks on card skimmer scam prevention

06/07/23: Eight arrested in connection to a diesel fuel theft ring, eight still at large, police say

01/12/23: Most credit card skimmers recovered in Houston, $50 million of fraud prevented

10/27/22: How to spot credit card skimmers hidden inside grocery stores, ATMs and gas stations

04/22/22: Texas Financial Crimes Intelligence Center sees success in first several months of operation

Florida also operates a Financial Crime Analysis Center (FCAC) within its Department of Law Enforcement's Office of Statewide Intelligence. Established in 2000, FCAC's mission is to "proactively research financial intelligence to reveal trends, patterns or correlations indicative to money laundering, terrorist financing or any criminal activities that threaten the state of Florida."[619] FCAC also supports state and local law enforcement agencies by conducting research and analysis of financial data filed under the Bank Secrecy Act.[620]

Local task forces focused on elder financial fraud have also emerged as an important model. The San Diego Elder Justice Task Force has been cited as a successful model for aggregating individual elder fraud cases into larger coordinated prosecutions—allowing local law enforcement to bring resources and prosecutorial strategies that match the scale of organized fraud operations.[621] This Task Force, which was created in 2020, "for the first time, combined investigative resources and critical data sharing from federal, state, and local authorities."[622] Key participants include the FBI, the U.S. Attorney's Office, the District Attorney's Office, as well as other state and local government representatives.[623] As of 2025, the Task Force had "tracked or

---

[618] *FCIC in the News*, TX. FIN. CRIMES INTEL. CTR., https://fcic.texas.gov/ (last visited July 1, 2026).
[619] *Financial Crime Analysis Center*, OFF. OF STATEWIDE INTELL., FL. DEP'T OF LAW ENF'T, https://www.fdle.state.fl.us/osi (last visited July 1, 2026).
[620] *Id.*
[621] *Elder Fraud: Task Force in San Diego Shows How Collaboration is a Key Tool in Fight Against Scammers*, FED. BUREAU OF INVESTIGATION (May 19, 2023), https://www.fbi.gov/news/stories/elder-fraud-task-force-shows-how-collaboration-is-a-key-tool-in-fight-against-scammers.
[622] Press Release, Off. of the Dist. Att'y of the Cty of San Diego, *supra* note 37.
[623] *Id.*

identified more than 4,600 victims and over $325 million in losses [to elder fraud and scams] in San Diego County."[624]

D. Consumer Education Efforts

Across both government and private sector, entities have significantly expanded their investment in consumer education. In fact, every stakeholder with whom Committee staff engaged stressed that—even though not a solution in itself—informed consumers represent one of the most cost-effective defenses against fraud and scams.[625] Ms. Kate McKune, General Counsel of Park Community Credit Union, also stressed the importance of education in front of the Subcommittee on Financial Institutions:

> We see [education] as an essential piece of how we are protecting our consumers. We absolutely have to have educated consumers because many times . . . there is so much shame involved in admitting that you have been scammed. That is one layer of the problem. . . . [The other layer is that] they call it social engineering for a reason. These are manipulations of people's vulnerabilities and the things they worry most about. And so, if we are in a position where they are not going to answer our questions, they are not going to tell us what is happening, the best tool we have, really, the very first tool has to be fundamental understanding and sophistication in consumers about the risks of fraud."[626]

Individual companies have developed their own consumer education programs alongside industry-wide campaigns. For example, major banks regularly publish fraud alerts, scam awareness content, and "Know Your Rights" guides for customers.[627] These materials are disseminated via multiple vectors, including through mobile banking apps, email communications, ATM screens, branch materials, and social media.[628] Tech companies have taken a similar approach. For example, Google has invested in educational content for users about recognizing phishing, fake ads, and impersonation attempts.[629] Meta likewise leverages warning labels on suspicious content, in-app alerts when users are about to send money to new contacts, and educational pop-ups targeting common scam patterns to inform customers about potential fraud schemes and scams.[630]

Public sector agencies have also developed their own consumer education efforts. For example, the Federal Reserve's Consumer Help Center provides educational content on banking rights, complaint processes, and fraud prevention. The Federal Deposit Insurance Corporation (FDIC) operates an extensive financial literacy program that includes fraud prevention guidance. FinCEN also engages in public outreach by publishing alerts that often describe a certain threat

---

[624] *Id.*
[625] Briefings with Committee Republican Staff (notes on file with the Committee).
[626] *Fighting Fraud on the Front Lines*, *supra* note 43 (statement of Kate McKune, General Counsel, Park Community Credit Union, on behalf of America's Credit Unions).
[627] *See supra* Public and Private Sector Entities Have Taken Some Steps to Mitigate the Rise in Fraud and Scams.
[628] *Id.*
[629] *See Tips and Tools to Help You Stay Safer Online*, GOOGLE SAFETY CTR., https://safety.google/intl/en_us/safety/security-tips/ (last visited July 2, 2026).
[630] *See, e.g., Proactive Safeguards: How We're Protecting You from Scams*, SCAM PROTECTION CENTER, META, https://www.meta.com/safety/scam-protection-center/safety-tips/proactive-safeguards (last visited July 1, 2026).

typology.[631] FinCEN publishes these alerts via their website. Although these alerts are available to the broader public, financial institutions tend to be the target audience.[632] Similarly, the National Credit Union Administration (NCUA) issues publications that discuss some cybersecurity scams, such as the Money Basics Guide for Savings and Checking Accounts, which touches on phishing and pharming scams.[633] It has also issued videos, blog posts, and webinars all focused on bringing awareness to fraud and scams.[634]

Other examples of campaigns and materials from government agencies and market participants are highlighted below.

<u>Government Agencies</u>

- *Federal Reserve Toolkits.* In August 2025, the Federal Reserve released "two online toolkits for scams and check fraud mitigation."[635] These "toolkits are intended to support education and increase awareness about scams and check fraud, enable the payments industry to better identify and fight them, and foster industry collaboration on fraud and scams mitigation." [636] Both toolkits provide information on the basics of scam and check fraud, as well as tactics used and scenarios for consumer awareness.[637]

- *SEC Investor Education Website & Other Efforts.* The SEC also maintains investor.gov, a comprehensive investor education website that provides plain-language explanations of investment products, red flags to watch for, and specific guidance on common scam types including "relationship investment scams."[638] The site is a primary consumer-facing resource for investment fraud education and is updated as new scam typologies emerge.[639] Beyond the website, the SEC's Office of Investor Education and Assistance (OIEA) leads investor education events, produces investor alerts and bulletins, and monitors an investor complaint form wherein an individual can report an issue with an investment account or the firm or individual managing it.[640]

---

[631] Briefings with Committee Republican staff (notes on file with Committee).
[632] Briefings with Committee Republican staff (notes on file with Committee).
[633] Briefings with Committee Republican staff (notes on file with Committee).
[634] Briefings with Committee Republican staff (notes on file with Committee).
[635] News Release, Bd. of Governors of the Fed. Rsrv. Sys., Federal Reserve unveils two online toolkits for scams and check fraud mitigation (Aug. 14, 2025) https://www.frbservices.org/news/fed360/issues/081425/industry-perspective-toolkits-scams-check-fraud-mitigation.
[636] *Id.*
[637] *See Scams Mitigation Toolkit*, BD. OF GOVERNORS OF THE FED. RSRV. SYS., https://fedpaymentsimprovement.org/resources/scams-mitigation-toolkit/ (last visited July 1, 2026); *Check Fraud Mitigation Toolkit*, BD. OF GOVERNORS OF THE FED. RSRV. SYS., https://fedpaymentsimprovement.org/resources/check-fraud-mitigation-toolkit/ (last visited July 1, 2026).
[638] *Investor.gov*, SEC. & EXCH. COMM'N, https://www.investor.gov/ (last visited July 1, 2026).
[639] *Id.*
[640] *About, Office of Investor Education and Assistance*, SEC. & EXCH. COMM'N, https://www.sec.gov/about/divisions-offices/office-investor-education-assistance (last visited July 1, 2026).

- *FTC's Pass It On & Other Campaigns.* Since 2014, the FTC has operated its "Pass It On" campaign, through which it provides toolkits and materials for consumers. The toolkits cover more than a dozen common scam categories, ranging from impersonation and romance scams to home repair fraud, fake prize schemes, and tech support scams.[641] FTC's materials are available in multiple languages and formats, and they are distributed free of charge.[642] Beyond Pass It On, the FTC maintains a comprehensive consumer education infrastructure. Its consumer.ftc.gov website publishes ongoing scam alerts, trend reports, and plain-language guidance.[643]

- *FBI's Take a Beat Campaign.* Launched in 2024, this campaign sough to "raise awareness of the frauds and scams impacting the public and encourage reporting to law enforcement."[644] The FBI highlights common fraud and scam typologies, recommendations for preventing losses, and describes how victims can report.

- *U.S. Postal Service Inspection Service Messaging.* The U.S. Postal Service's Inspection Service is among the most prolific of government agencies in terms of consumer education. It runs annual public service announcements, the 2025 version of which received over six million views.[645] It also circulates internal prevention messaging focused on employee safety and crime prevention.[646] These efforts are disseminated across various platforms, including on social media, traditional media, and partnerships with industry and other law enforcement agencies.[647]

Market Participants

- *ABA's #BanksNeverAskThat and #PracticeSafeChecks Campaigns.* ABA has two separate, but complementary, educational campaigns aimed to bring awareness to common fraud and scams schemes. Its #BanksNeverAskThat campaign is an anti-phishing campaign that highlights common ways scammers impersonate banks.[648] In 2025, ABA added the theme of "Snap Out of It!," which was designed to address the psychological manipulation tactics scammers use, such as manufactured urgency, false authority, and emotional pressure, to help consumers recognize and break free from the trance-like state that makes these tactics effective.[649] ABA's #PracticeSafeChecks campaign addresses the surge of check fraud by encouraging

---

641 *Pass It On*, FED. TRADE COMM'N, https://consumer.ftc.gov/features/pass-it (last visited July 1, 2026).
642 *Id.*
643 *See Consumer Advice*, FED. TRADE COMM'N, https://consumer.ftc.gov/ (last visited July 1, 2026).
644 Press Release, Fed. Bureau of Investigation, FBI Announces Nationwide 'Take A Beat' Campaign to Increase Awareness of Frauds and Scams (Aug. 19, 2024), https://www.fbi.gov/news/press-releases/fbi-announces-nationwide-take-a-beat-campaign-to-increase-awareness-of-frauds-and-scams.
645 Briefings with Committee Republican staff (notes on file with the Committee).
646 Briefings with Committee Republican staff (notes on file with the Committee).
647 Briefings with Committee Republican staff (notes on file with the Committee).
648 *See Banks Never Ask That*, AM. BANKERS ASS'N, https://www.banksneveraskthat.com/ (last visited July 1, 2026).
649 Press Release, Am. Bankers Ass'n, ABA, America's Banks Relaunch #BanksNeverAskThat and #PracticeSafeChecks Campaigns to Help Consumers Spot Scams (Oct. 1, 2025), https://www.aba.com/about-us/press-room/press-releases/bnat-launch-2025.

consumers and small businesses to adopt digital payment options and use checks safely when they must.[650]

- *Financial Institution Campaigns.* Throughout 2026, Bank of America is hosting "scaminars"—seminars focused on scam and fraud prevention awareness.[651] These programs "[aim] to strengthen the financial wellness of [customers] through greater accessibility to fraud and scam prevention training."[652] JPMC has similarly held educational workshops focused on educating consumers to recognize common scam indicators.[653] JPMC has also taken a unique and innovative step by employing behavioral psychologists to help hone JPMC's consumer education messaging and to engage with fraud/scam victims.[654] As it relates to the latter, a "team of skilled associates reaches out to connect with clients, providing support during stressful and impactful moments, and works to stop scams in real time."[655]

- *Credit Union Videos.* The Maine Credit Union League launched a statewide collaboration with the Maine Attorney General's Office, Maine State Police, Maine Bureau of Financial Institutions, and fraud investigators to produce a video with clear actionable steps viewers can take to prevent fraud and scams.[656] Research indicates that such efforts can be effective in helping customers identify fraudulent schemes—while retaining the ability to identify genuine investment opportunities.[657]

- *Google's Be Scam Ready game.* In 2025, Google launched an interactive game focused on making consumers "scam ready."[658] "Be Scam Ready is a hands-on game that lets [individuals] experience scammers' tactics firsthand, helping [them] build the gut instinct to shut fraud down instantly."[659] As part of the efforts, Google provides important reminders, including "question the 'easy entry,'" "slow down, don't fall for urgency," and "verify scarcity claims and offers."[660]

---

[650] *See Practice Safe Checks*, AM. BANKERS ASS'N, https://www.practicesafechecks.com/ (last visited July 1, 2026).
[651] Newsroom, Bank of Am., Bank of America to Host Thousands of "Scaminars" to Help Protect Clients and Fight Fraud (June 15, 2026), https://newsroom.bankofamerica.com/content/newsroom/press-releases/2026/06/bank-of-america-to-host-thousands-of--scaminars--to-help-protect.html.
[652] *Id.*
[653] News release, JPMorganChase, JPMorganChase Announces Largest Financial Fraud and Scam Prevention Effort in Firm's History (Nov. 17, 2025), https://media.chase.com/news/jpmc-announces-largest-financial-fraud-and-scam-prevention-effort-in-firms-history.
[654] *Id.*
[655] *Id.*
[656] *ICBA releases new check fraud guide*, INDEP. CMTY. BANKERS OF AM. (Nov. 22, 2024), https://www.icba.org/w/icba-releases-new-check-fraud-guide.
[657] Jeremy Burke et al., *Can Educational Interventions Reduce Susceptibility to Financial Fraud?,* FINRA INV. EDUC. FOUND. (Mar. 2021), https://www.finrafoundation.org/sites/finrafoundation/files/2024-10/can-educational-interventions-reduce-susceptibility-to-financial-fraud_0_0.pdf.
[658] Briefings with Committee Republican staff (notes on file with the Committee); *Be Scam Ready*, GOOGLE, https://bescamready.withgoogle.com/intl/en (last visited July 1, 2026).
[659] *Be Scam Ready*, GOOGLE, https://bescamready.withgoogle.com/intl/en (last visited July 1, 2026).
[660] *Id.*

- *Visa's Biannual Threat Report.* Visa issues both a confidential and a public biannual threats report, which "draws on intelligence from Visa's global network."[661] The reports highlight trends in fraud and scams, including developments in the use of technology.[662]

- *AARP Materials*. AARP produces extensive free publications, online tools, and in-person workshops for individuals, families, and caregivers. The organization has built a content library covering identity theft, romance scams, investment fraud, tech support scams, grandparent scams, and many other fraud types, with materials specifically tailored to the experiences and communication preferences of older adults.[663] It also releases a bi-weekly fraud newsletter[664] and maintains a "Scam Map," through which individuals can see fraud and scams reported near them[665].

DESPITE THESE EFFORTS, SIGNIFICANT BARRIERS TO MITIGATING FRAUD AND SCAMS REMAIN

Despite the efforts noted above, the prevalence and impact of the illegal schemes demonstrate that gaps remain. As criminals adapt their tactics, once novel approaches will quickly join the ranks of being outdated, slow tools that put businesses and governments further behind.[666] Throughout their work, Committee Republicans heard from numerous public and private stakeholders about barriers that serve as significant impediments to strengthening anti-fraud and scam efforts. Other impediments became clear when analyzing efforts across industries and agencies. Key examples of these barriers are discussed in more detail below.

A. Destigmatizing Victimization

When most people picture the victim of a serious crime, they imagine someone who elicits immediate sympathy—a survivor of violence or a person whose suffering is self-evidently not their fault. Fraud and scam victims often are not provided with the same compassion. Instead, they frequently face the assumption that they should have known better. In one survey, respondents cited "emotional distress" as the worst consequence of a scam—above financial loss.[667]

This shame is a major amplifier of the psychological impact fraud and scams have. Scam victims often experience severe emotional distress, including depression, anxiety, shame, embarrassment, and post-traumatic stress disorder.[668] According to a recent GASA study, "69

---

661 *See, e.g.*, Press Release, Visa, Visa Threats Report: As Network Security Strengthens, Criminals Accelerate Shift to AI-Enabled Social Engineering (May 20, 2026), https://corporate.visa.com/en/sites/visa-perspectives/newsroom/visa-spring-2026-biannual-threats-report.html.
662 *See, e.g.*, *id.*
663 *See Scams & Fraud*, AARP, https://www.aarp.org/money/scams-fraud/ (last visited July 1, 2026).
664 *See About Fraud Watch Network*, AARP, https://www.aarp.org/money/scams-fraud/about-fraud-watch-network/ (last visited July 1, 2026).
665 *See Scam Tracking Map*, AARP, https://www.aarp.org/money/scams-fraud/tracking-map/ (last visited July 1, 2026).
666 ASPEN INST., UNITED WE STAND, *supra* note 282, at 10.
667 *2025 State of Scams Report*, ALLOY (2025), https://www.alloy.com/reports/2025-scams-report#emotional.
668 Balcombe, *supra* note 40.

[percent] of victims reported severe stress after a scam, 17 [percent] lost self-confidence, and 14 [percent] experienced family tensions. They are people who have stopped sleeping, who no longer trust anyone, [and] who carry shame and guilt."[669] Romance scams are particularly emotionally damaging, with victims reporting feelings of marginalization and deep emotional shifts that hinder self-regulation, occasionally leading to suicidality.[670]

This dynamic—the internalized and externally reinforced shame of having been deceived—often results in victims choosing to stay silent, rather than report the crimes they experienced.[671] Estimates of the extent of underreporting varies. At least one source estimates that just seven percent of scams are reported globally.[672] The Aspen Institute estimates that only 25 percent of victims file reports with law enforcement, with the others citing "shame and hopelessness as reasons for not seeking help from authorities," among others.[673] Shame, in other words, is not just a personal problem for individual victims. It is a structural problem that systematically distorts our understanding of fraud's true cost. Silence also damages fraud prevention tactics, law enforcement efforts, and public awareness campaigns. When victims choose not to report, law enforcement loses the data it needs to identify patterns, build cases, and bring criminal networks down. Prosecutors cannot charge individuals they do not know about; banks cannot flag emerging scam methodologies they have not been alerted to; policymakers cannot allocate resources to a problem whose true scale remains hidden.

Modern scams are precision instruments designed by criminal organizations specifically to exploit universal human characteristics. These vulnerabilities should not elicit blame. And although victims may not report for a variety of reasons, shaming victims creates a self-reinforcing cycle that lets criminal networks operate with near impunity. Therefore, it is imperative that society must first counteract the stigma associated with scam victimization, working to reduce—and if possible eliminate—the negative social and emotional outcomes experienced by scam victims.[674] In doing so, the various stakeholders charged with combating these criminals will have better data and understanding of the true nature of the crimes, and the victims themselves will hopefully find supportive systems to help them through what is likely to be one of the more difficult experiences they face in life.

B. Coordinating Consumer Education

Although proactive and preventative measures are needed, potential victims must be on guard for fraud and scam attacks. Fraud is, in large part, a knowledge problem. Scammers succeed because victims do not recognize what is happening until it is too late. The solution to a knowledge problem is education—but only if that education reaches people before the scam is

---

[669] Sissi De La Pena, *The Industrialization of Deception: Why 2026 Will Be the Year Cyber Scams Change Forever*, GLOBAL ANTI-SCAM ALLIANCE (Mar. 10, 2026), https://gasa.org/knowledge-base/blog/the-industrialization-of-deception-why-2026-will-be-the-year-cyber-scams-change-forever.
[670] Balcombe, *supra* note 40.
[671] Matt Alderton, *How and Where to Report Scams – and Why It's Crucial to Do So*, AARP (Dec. 29, 2025), https://www.aarp.org/money/scams-fraud/where-to-report-scams/?msockid=2b25242999fa650235ab31e8985d64c0.
[672] *Scam Intelligence & Impacts Report 2025*, F-SECURE (2025), https://www.f-secure.com/i/x/6a979e8a7d/2025-09-24_scam-report.pdf.
[673] ASPEN INST., UNITED WE STAND, *supra* note 282, at 7.
[674] *Id.* at 57.

delivered, in a form they trust, reinforces its messages over time, and is built around a deep understanding of how fraud actually works and how human psychology actually processes risk.

Both private industry and government recognize the importance of consumer education. As described above, practically every stakeholder with which Committee staff engaged highlighted alerts, notices, reminders, mailings, webinars, and other ways in which they communicate with consumers about fraud and scams.[675] As explained above, stakeholders regularly publish education campaigns: the ABA runs its #BanksNeverAskThat campaign; the AARP publishes materials; and government agencies issue public service announcements.[676] Individual banks, telecommunications companies, technology platforms, and nonprofit organizations also each produce their own consumer-facing educational content, usually designed in isolation, released without coordination, and measured—if at all—against their own internal benchmarks rather than any shared national standard.[677]

The issue with this approach, however, is that it results in a consumer education landscape that is simultaneously everywhere and nowhere—dozens of well-intentioned campaigns speaking in dozens of different voices, with no unified message, no shared identity, no coordinated media strategy, no single point of contact, and no way to evaluate whether any of it is working. Public awareness campaigns on fraud and scams are currently fragmented across agencies, with no coordinating authority and no consistent national message.

Take a consumer who views ABA's content, then attends an FTC webinar, then listens to their Congress member's townhall, and then sees an ad for National Fraud Month. That one consumer has engaged with four different messages, four different slogans, four different calls to action, and likely, four different reporting destinations. The cumulative effect of fragmented messaging is not four times the awareness—it is confusion, in a competitive media environment where scammers themselves produce highly polished, targeted, and psychologically sophisticated communications. Without centralized leadership, enforcement and regulatory actions remain fragmented. The same is true of the consumer education landscape.

What is needed instead is a coordinated national consumer education campaign on fraud and scams, conceived at a national scale, executed across every major communications channel, and sustained over the years to produce lasting behavioral change. In conversations with stakeholders, the most commonly referenced model was the "Smokey Bear" campaign.[678] Other examples included the "Click It or Ticket" seatbelt campaign and the post-September 11 "If You See Something, Say Something" campaign. In all these instances, the sustained, coordinated, multi-channel public safety messaging had measurable behavioral change at population scale. Each of these campaigns had a unified brand, a consistent message, sustained funding, and a coordinated strategy that aligned government agencies, private-sector partners, and community organizations around a shared framework.

In thinking about fraud and scams, it is important to keep in mind the vast breadth of both types of schemes and the individuals victimized. Any effective public campaign should not

---

[675] *See supra* Public and Private Sector Entities Have Taken Some Steps to Mitigate the Rise in Fraud and Scams.
[676] *See id.*
[677] *See id.*
[678] Briefings with Committee Republican staff (notes on file with the Committee).

deliver the same message to every audience—it must be segmented by demographic, vulnerability, and exposure risk, and tailored accordingly. In other words, although messages should share a common identity, a national campaign would need to develop specific, evidence-based content for each major scam typology and each major target population, rather than producing a one-size-fits-all message that serves no one particularly well. Properly focused consumer education can help members of the public spot potential scams and be wary of certain types of communications and messages.[679]

One of the most consistent findings in research is that the effects of fraud education interventions decay without reinforcement.[680] Thus, a national campaign must be conceived as a multi-year commitment—like anti-smoking campaigns that ran for decades—with consistent core messages sustained through regular content updates that address the newest scam tactics. Scammers evolve their methods rapidly; a campaign that teaches consumers only to avoid last year's fraud techniques will be outpaced within months.

C. Creating a Cohesive Reporting Mechanism

Timely consumer reporting about actual or suspected scam activity is one of many tools to prevent the spread of scams and reduce harm. However, in addition to the shame described above, many victims choose not to report simply because they do not know where to report.[681] A recent survey of over 5,000 U.S. adults found that 58 percent of those surveyed opted not to report because of "uncertainty about where to report."[682] A victim who has just lost money in a fraud or scam faces an immediate and daunting question: who do I tell? The answer, it turns out, depends on what kind of scam it was, how the money was sent, where the scammer might be located, whether a business was involved, whether a government program was impersonated, and the demographics of the victim. It is not an easy set of questions to answer, and evidence shows that millions of Americans simply give up without reporting at all.[683] In fact, as one individual reported in response to survey:

> The reporting process isn't convenient. And it also isn't . . . widely familiar. I wouldn't know who to go to. I would look it up. Who do I report this to? . . . And so that probably contributed to the reason I didn't report [a scam].[684]

At the federal level alone, there are no fewer than a dozen distinct agencies and portals that receive fraud or scam complaints, each with its own jurisdiction, intake form, and purpose.

---

[679] ASPEN INST., UNITED WE STAND, *supra* note 282, at 57.
[680] SCAMS AGAINST OLDER ADULTS ADVISORY GROUP, A REVIEW OF SCAM PREVENTION MESSAGING RESEARCH: TAKEAWAYS AND RECOMMENDATIONS 4 (2024); Jeremy Burke et al., *supra* note 657.
[681] Michael LaFleur, *Why Underreporting Holds Back Fraud Prevention*, THREATMARK (Feb. 7, 2025), https://www.threatmark.com/why-underreporting-holds-back-fraud-prevention/.
[682] *See* UNITED STATES OF SCAMS, *supra* note 10, at 23.
[683] LaFleur, *supra* note 681; FED. TRADE COMM'N, PROTECTING OLDER CONSUMERS 2022-2023 39 (Oct. 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p144400olderadultsreportoct2023.pdf (noting that many people do not report crimes).
[684] *See* UNITED STATES OF SCAMS, *supra* note 10, at 23.

This includes the Treasury Department,[685] FBI,[686] FTC,[687] and Social Security Administration,[688] among others. The NCUA, for its part, maintains a dedicated page through which credit union customers can report fraud and scams, and it also runs a fraud hotline.[689] Beyond the federal level, local and state law enforcement, including many state attorneys general offices, maintain their own systems for reporting fraud and scams. Given all scams are different and involve different agencies and types of firms—both financial and non-financial—an individual might have to reach out to a number of local, state, and federal agencies depending on the situation.[690] That places a burden on people who are likely distressed and unfamiliar with the distinctions between federal regulatory jurisdictions.

The solution most clearly implied is a cohesive reporting mechanism that allows complaints to be centrally reported and routed efficiently to the appropriate agencies. Such a system would not only assist victims in coming forward, but it would also help synthesize data collection, thereby creating more accurate measures of the prevalence of fraud and scams. As noted above, accurate data is important for consumers and households, businesses, law enforcement, and policymakers. A robust measurement system can reveal where progress is being made in combating fraud and scams and where reprioritization is needed, ultimately improving outcomes for individuals, businesses, and the economy as a whole.[691] The fact is: the bifurcated avenues to report fraud and scams and the difficult-to-navigate reporting maze will continue to serve the interests of scammers far more than it serves the victims.

D. <u>Forming a Unified Government Approach</u>

If there is universal agreement on one thing, it is that no individual, business, agency, or entity can solve fraud and scams on their own. As described above, a whole-of-ecosystem approach is needed—one that brings together private industry and public sector, across the federal, state, and local levels.

At the government level, however, more must first be done to harness and amplify the resources and efforts that are currently occurring. Agencies from the DOJ[692] and Treasury,[693] to

---

685 *Report Fraud Waste and Abuse*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/services/report-fraud-waste-and-abuse (last visited July 1, 2026).
686 *File a Complaint with Us*, INTERNET CRIME COMPLAINT CTR., https://www.ic3.gov/ (last visited July 1, 2026)..
687 *Report Fraud*, FED. TRADE COMM'N, https://reportfraud.ftc.gov/ (last visited July 1, 2026).
688 *Fraud Prevention and Reporting – How to Report Fraud*, SOCIAL SEC'Y ADMIN., https://www.ssa.gov/fraud/.
689 *MyCreditUnion.gov*, NAT'L CREDIT UNION ADMIN., https://mycreditunion.gov/ (last visited July 1, 2026); briefing with Committee Republican staff (notes on file with the Committee).
690 *Cf. Fraud and Scams*, CONSUMER EDUCATION, CONSUMER FIN. PROTECTION BUREAU (Sep. 5, 2025), https://www.consumerfinance.gov/ask-cfpb/i-think-i-or-someone-i-know-was-the-victim-of-a-scam-or-financial-exploitation-who-can-i-contact-for-help-en-1777/.
691 ASPEN INST., UNITED WE STAND, *supra* note 282, at 41.
692 Press Release, U.S. Dep't of Just., Departments of Justice and Homeland Security Partnering on Cross-Agency Trade Fraud Task Force (Aug. 29, 2025), https://www.justice.gov/opa/pr/departments-justice-and-homeland-security-partnering-cross-agency-trade-fraud-task-force; *see also* Press Release, U.S. Dep't of Just., New Scam Center Strike Force Battles Southeast Asian Crypto Investment Fraud Targeting Americans (Nov. 12, 2025), https://www.justice.gov/usao-dc/pr/new-scam-center-strike-force-battles-southeast-asian-crypto-investment-fraud-targeting.
693 Treasury Sanctions Southeast Asian Networks, *supra* note 275.

the FCC[694] and the FTC,[695] and many others, all have critical roles in combating fraud. Although many of these agencies are making an effort to address the growing rise in fraud and scams, no agency has made this issue its top priority or led on leading on creating a cross-government initiative. As described above, some agencies do—either formally or informally—collaborate with other agencies, but there is currently no "government-wide strategy to guide [these] efforts."[696] In fact, as GAO has found, "no agency is mandated or required to [prioritize combating fraud and scams], either individually or collectively."[697] Consequently, "no agency has taken the lead [on] a comprehensive . . . strategy to help guide the various activities agencies employ to counter scams and mitigate the risk for potential fragmentation and overlap."[698]

The existing fragmentation of agencies' efforts to counter fraud and scams "risks diminishing their efficiency and effectiveness."[699] As detailed above, the Trump Administration has taken several steps to better address fraud and scams. Nevertheless, agencies are largely operating on an informal basis, with fraud and scams failing to be the top priority. This can result in an "uncoordinated and unfocused" approach.[700] To date, "the United States has not yet articulated a national plan for combating scams, even as the threat keeps growing."[701] There is no government-wide strategy guiding existing efforts to combat fraud.[702] Without such a coordinated effort, the United States will continue to risk "fragmentation of effort or overlap of multiple activities" that serves to limit the effectiveness and impact of any administration's efforts.[703]

Importantly, the Trump Administration has shown that it can—and is willing to—create government-wide strategies to address important challenges harming Americans. For example, on March 16, 2026, President Trump signed Executive Order 14395, establishing the Task Force to Eliminate Fraud.[704] Despite the name invoking the general term of fraud, the Task Force has a fundamental limitation baked into its design: it is narrowly focused on fraud in federal government benefit programs.[705] Committee Republicans believe the Task Force's concept could be easily expanded or mirrored for financial fraud and scams. The Task Force has already demonstrated that focused executive attention, combined with institutional authority and interagency coordination, can produce results that years of fragmented agency-by-agency enforcement could not. Expanding the scope of the current Task Force to include fraud and

---

694 *Consumer Complaints*, FED. COMMC'NS COMM'N, https://consumercomplaints.fcc.gov/hc/en-us (last visited June 23, 2026).
695 *Scams*, FED. TRADE COMM'N, https://consumer.ftc.gov/scams (last visited Dec. 2, 2025).
696 GAO-25-107088, *supra* note 26, at 15.
697 *Id.* at 30.
698 *See generally id.*
699 *Id.* Fragmentation refers to those circumstances in which more than one federal agency (or more than one organization in an agency) is involved in the same broad area of national need, and opportunities exist to improve service. U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-49SP, FRAGMENTATION, OVERLAP, AND DUPLICATION: AN EVALUATION AND MANAGEMENT GUIDE 20-21 (2015) [hereinafter GAO-15-49SP].
700 ASPEN INST., UNITED WE STAND, *supra* note 282, at 41.
701 *Id.* at 6.
702 GAO-25-107088, *supra* note 26.
703 GAO-25-107088, *supra* note 26; *see also* GAO-15-49SP, *supra* note 699.
704 Fact Sheet: President Donald J. Trump Establishes the Task Force to Eliminate Fraud, The White House (Mar. 16, 2026), https://www.whitehouse.gov/fact-sheets/2026/03/fact-sheet-president-donald-j-trump-establishes-the-task-force-to-eliminate-fraud/.
705 *Cf. id.*

scams or creating a similar Task Force would not only bring cohesion and accountability, but it would send a signal that this is a top priority for the Administration.

E. Using Consistent Terminology

As explained above, fraud and scams share many similarities and are often referred to interchangeably. Yet, certain statutes and regulations draw a distinction—particularly in terms of liability. The absence of a uniform, cross industry definition of what constitutes a "fraud" versus a "scam" creates inconsistent reporting, complicates liability determinations, and fosters an inability to accurately quantify the full scope of harms to consumers. Every individual, business, and agency affected by fraud and scams must be a part of any effective solution, but definitional inconsistency prevents the coordinated response the problem demands.

At its core, different industries and government agencies define fraud and scams differently to serve their own regulatory and operational purposes, without reference to a common standard. Financial institutions and their regulators, for example, employ the distinction between an unauthorized fraud and an authorized scam to determine liability exposure under Reg E.[706] Federal agencies that collect complaints, publish data, and pursue enforcement actions—such as the FTC, FCC, and others—do so without distinction.[707] The result is that the same underlying harm to consumers may be characterized differently depending on which institution or agency is reporting it.

The lack of a common taxonomy similarly impedes both private-sector information-sharing and interagency coordination. Financial institutions, technology platforms, telecommunications carriers, and federal agencies that might otherwise share intelligence about emerging fraud patterns are constrained when operating under different definitions. Payment platforms that could alert financial institutions to emerging scam patterns may hesitate when uncertain whether their conduct constitutes "fraud" triggering regulatory reporting obligations or a "scam" falling outside their remit. Every player in the fraud and scams ecosystem must be part of the solution, and that responsibility is difficult without a shared vocabulary.

F. Better Sharing of Information

Fraud is a collaborative enterprise. Criminal networks communicate in real time across encrypted channels, update their methods within hours of encountering a new countermeasure, and transfer lessons learned from one operation to the next with extraordinary speed. The institutions trying to stop these networks—banks, telecommunications companies, technology platforms, law enforcement agencies, and government regulators—largely do not. With some exceptions, they operate in silos, bound by legal constraints, competitive instincts, jurisdictional boundaries, and legacy frameworks that were never designed with the scale or sophistication of modern fraud in mind. The result is a fundamental asymmetry: criminals collaborate freely while defenders are left to largely fight alone. As Ms. Jacqueline Burns Koeven emphasized in a

---

[706] Kenneth Benton, *Consumer Liability for Unauthorized Transactions Under the Electronic Fund Transfers Act and Regulation E*, CONSUMER COMPLIANCE OUTLOOK, https://www.consumercomplianceoutlook.org/2025/third-issue/consumer-liability/ (last visited May 26, 2026).
[707] GAO-25-107088, *supra* note 26.

hearing in front of the Subcommittee on National Security, Illicit Finance, and International Financial Institutions:

> [T]he current reality is that scammers are exploiting the siloed nature of how the public and private sector identify and respond to these schemes. Scammer syndicates are organized and agile, and they are capitalizing on our visibility gaps. Today, scam victims have multiple state, local, and federal agencies they can report to, yet there is no easy mechanism for these agencies to share with each other. . . . And financial institutions reporting on scams have no visibility into the scams reported by their peers, leaving them unable to protect their customers from scams known to the government or the financial institutions next door.[708]

Eliminating that asymmetry is among the most important systemic reforms to enhance fraud prevention.

Each sector has a piece of the puzzle, but none has the full picture. Banks can see fraudulent transactions but cannot see the scam text messages, false advertisements, or social media messages that preceded them. Moreover, modern fraud and scams—particularly account takeovers, synthetic identity fraud, money-mule networks, authorized push-payment scams, and check fraud—typically involves activity that spans multiple banks and payment channels.[709] A single institution often sees only a fragment of the pattern. Telecommunication companies can see the scam calls but cannot see where the money went. Technology platforms can see the fake profiles but cannot see the bank accounts they drain. Law enforcement can see different aspects but lack the real-time data that private industry holds. Effective detection therefore requires identifying linkages across accounts, devices, typologies, and transaction flows that no one institution can observe in isolation.[710]

Practically every stakeholder with which Committee staff engaged highlighted the need for better information-sharing across both the public and private sectors, with many stakeholders stating the lack of information sharing is the biggest hindrance to their fraud and scam efforts.[711] These stakeholders acknowledge that progress is being made, but more must be done. They stressed that legal and regulatory risks prohibit or dissuade real-time information sharing across industries.[712] For example, one stakeholder in the telecommunication industry pointed to historical FCC regulatory enforcement actions in which companies were fined for sharing information with other companies.[713] According to this stakeholder, unless the law explicitly

---

[708] *Following the Money*, *supra* note 41 (statement of Ms. Jacqueline Burns Koeven, Head of Cyber Threat Intelligence, Chainanalysis).
[709] *See* Greg Williamson & Drew Ruben, *What Works, What Doesn't in the Global Fight Against Scams*, BANK POL'Y INST., (Feb. 4, 2026), https://bpi.com/what-works-what-doesnt-in-the-global-fight-against-scams/ (discussing how fraud proceeds traverse multiple accounts and channels, including mule networks).
[710] Andrea Dal Pozzolo et al., *Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy*, 11 IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS 25 (2019), https://ieeexplore.ieee.org/document/8038008 (noting that multi-feature, networker behavioral analysis can significantly improve fraud detection performance compared to siloed transaction analysis).
[711] Briefings with Committee Republican staff (notes on file with the Committee).
[712] ASPEN INST., UNITED WE STAND, *supra* note 282, at 26.
[713] Briefings with Committee Republican staff (notes on file with the Committee).

allows for information sharing, many companies determine that the legal and regulatory risks outweigh the potential benefits that could result for customers.[714]

The *Bank Secrecy Act* (BSA) framework allows financial institutions to file SARs, while prohibiting disclosure of SARs or information that would reveal their existence.[715] In addition, section 314(b) of the *USA PATRIOT Act*[716] permits voluntary information sharing among financial institutions to identify and report activities involving money laundering or terrorist activity.[717] On June 12, 2026, FinCEN issued guidance clarifying that certain fraud- and scams-related crimes—including but not limited to mail fraud, wire fraud, bank fraud, and securities fraud—constitute underlying predicate crimes of money laundering and thus are covered by 314(b).[718] The volume of financial institution information has not been lacking. On the contrary, in FY25 alone, more than 28 million BSA reports were filed with FinCEN, and over 1,690 financial institutions referenced 314(b) information sharing in SAR narratives.[719] However, FinCEN and law enforcement must work more effectively to connect the dots produced by this reporting. They must also improve their own information sharing with financial institutions through feedback loops that help those institutions understand which BSA information is actually useful.

The *Fair Credit Reporting Act* (FCRA) presents additional complexity. If a consortium aggregates consumer information and provides outputs used to make eligibility determinations, that entity could be characterized as a "consumer reporting agency,"[720] triggering extensive compliance obligations, accuracy standards, and private litigation exposure.[721] Even where fraud detection—not credit underwriting—is the purpose, the risk of inadvertently falling within FCRA's scope can create an obstacle for shared databases or cross-institution risk signals.

Competition law also discourages broad, structured data exchanges. The *Sherman Act*[722] and *Clayton Act*[723] prohibit anticompetitive agreements among competitors. While legitimate information exchanges can be lawful,[724] institutions are understandably risk-averse when considering the pooling of transactional or customer-level data, even for fraud-prevention purposes. Without explicit statutory safe harbors or regulatory oversight mechanisms, institutions carefully limit sharing to avoid potential antitrust exposure.

Beyond statutory constraints, supervisory expectations and model-risk governance standards create practical friction. Financial institutions, for example, must comply with safety-

---

[714] Briefings with Committee Republican staff (notes on file with the Committee).
[715] 31 U.S.C. § 5318(g).
[716] 31 U.S.C. § 5311 note.
[717] *Section 314(b) Fact Sheet*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/system/files/shared/314bfactsheet.pdf (last updated June 12, 2026).
[718] *Id.*
[719] FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FINCEN YEAR IN REVIEW: FISCAL YEAR 2025 (2026), https://www.fincen.gov/system/files/2026-05/FinCEN-Year-in-Review-2025.pdf
[720] 15 U.S.C. § 1681a(f).
[721] *See* 15 U.S.C. §§ 1681e(b), 1681i, 1681n, 1681o.
[722] 15 U.S.C. §§ 1, 2.
[723] 15 U.S.C. §§ 12-27.
[724] *See Maple Flooring Mfrs.' Ass'n v. United States*, 268 U.S. 563 (1925) (holding that trade associations do not violate the antitrust laws merely through sharing of information without concerted action to restrain competition).

and-soundness requirements under the *Federal Deposit Insurance Act*[725] and are subject to regulatory scrutiny regarding third-party risk management, data security, and model validation.[726] Without explicit interagency guidance supporting structured information-sharing utilities, smaller institutions may conclude that the operational and compliance risks outweigh the perceived benefits.

As a result, private companies today often rely on fragmented, bilateral exchanges or internal analytics to combat and prevent fraud.[727] Even where companies are willing to engage in such partnerships, negotiating the scope of the sharing can take months. At least one stakeholder informed the Subcommittee that a privacy agreement for an information sharing arrangement took more than six months to negotiate.[728] Criminal actors exploit these weaknesses. Fraud typologies routinely involve "mule" accounts opened at multiple institutions, rapid transfers across payment rails, and coordinated activity that is only visible when data is viewed holistically.[729] Modern analytics—including machine learning, network analysis, and behavioral modeling—are most effective when trained on diverse, cross-institutional datasets.[730] Without clearer legal pathways for controlled sharing, institutions cannot fully deploy these tools at scale.

As described above, several cross-sector information exchanges and public-private partnerships already exist, with new ones being launched every year. However, this runs the risk of creating too much noise in the system—with so many exchanges, potential participants are left not knowing which groups they should join. As the Aspen Institute has noted, "[t]o make informed decisions, industry actors need better visibility into the array of exchanges available to them, what distinguishes each exchange, any barriers to participation, and, ideally, reporting on their performance."[731] As private sector information exchanges become more standardized and government systems and standards become more modernized with improved coordination across agencies, it will be important that these systems are interoperable.[732] It will also be necessary for participants to understand what information must be shared to most effectively combat fraud and scams.

The path forward will require the federal government to provide, where necessary, statutory and regulatory guidance on cross-sector information sharing. As Mr. Joseph Schuster, a partner at Ballad Spahr with a specialty in advising clients on consumer financial services issues, emphasized in testimony before the Subcommittee on Financial Institutions:

---

725 12 U.S.C. § 1818.
726 *See, e.g.*, 12 C.F.R. Part 30.
727 *See* Heidi Bleau*, Regulatory Roadblocks to Fighting Financial Crime*, BIOCATCH (Oct. 30, 2024), https://www.biocatch.com/blog/regulatory-roadblocks-financial-crime (describing how current legal and operational constraints limit real-time information sharing to fight financial crime).
728 Briefings with Committee Republican staff (notes on file with the Committee).
729 Williamson & Ruben, *supra* note 709 (discussing how fraud proceeds traverse multiple accounts and channels, including mule networks).
730 *See, e.g.*, H.P. Josyula, *Fraud Detection in Fintech Leveraging Machine Learning*, RESEARCH SQUARE (Nov. 6, 2023), https://assets-eu.researchsquare.com/files/rs-3548343/v1/2c5c23de-876c-4ecf-87f8-b7b8b82d4dd4.pdf (noting that machine learning models benefit significantly from enriched and diverse datasets to improve fraud detection accuracy and robustness).
731 ASPEN INST., UNITED WE STAND, *supra* note 282, at 28.
732 *Id.* at 28-29.

> Fraud identification is inherently pattern recognition. The more information and data that you have, the easier it is to identify patterns that are abnormal. . . . If there were clarity or safe harbor under [the law] about sharing data for fraud or how that data could be shared, it would vastly improve financial institutions' and all these other companies' ability to share that data and have it available to prevent fraud.[733]

Mandatory cross-sector reporting framework could create consistent flows of intelligence from every sector to a central hub. Investment in interoperable technical infrastructure, so that signals from social media platforms, telecommunications providers, payment networks, and financial institutions can be combined in real time, would transform the speed and accuracy of fraud detection.

G. Promoting Flexibility for Financial Institutions

Financial institutions are required under Regulation CC (Reg CC)—which implements the *Expedited Funds Availability Act* (EFAA)—to make funds available to customers for certain types of deposits under certain specified timeframes. For example, financial institutions must make cash, wire transfers, government checks (including Treasury checks), cashier's checks, and certain other checks available on the first day following the banking day of deposit—often referred to as "next-day-availability."[734] Standard checks—such as a personal check from a family member or friend—must be made available by the second business day following the day of deposit with $275 available the next business day. Reg CC provides six exceptions that allow banks to extend deposit hold periods:

1. Checks deposited into accounts opened 30 or fewer days ago;
2. Large deposits greater than $6,725 but only for the amount *exceeding* $6,725;
3. Re-deposited checks;
4. Deposits made by checks to accounts that have been repeatedly overdrawn in the last six months;
5. Deposits of checks for which the bank doubts collectability; and
6. Deposits made under certain emergency conditions.[735]

Financial institutions must provide notices to customers when imposing extended holds on check deposits, and deposited funds are generally required to be available by the seventh business day after the deposit is made. Importantly, the six exceptions in Reg CC only allow for

[733] *Fighting Fraud on The Front Lines*, *supra* note 43 (statement of Mr. Joseph Schuster, Partner, Ballard Sphar LLP).
[734] 12 U.S.C. §§ 4001-4010.
[735] *Are there exceptions to the funds availability (hold) schedule?*, OFF. OF THE COMPTROLLER OF THE CURRENCY (June 2025), https://www.helpwithmybank.gov/help-topics/bank-accounts/funds-availability/funds-availability-exceptions.html.

extended holds for check deposits. Cash, wire transfers, or other electronic deposits such as ACH are not eligible for exception holds.[736]

The EFAA and Reg CC were enacted to address a very different set of risks than those confronting financial institutions today. At the time of adoption, check clearing was characterized by geographic delays, settlement uncertainty, and excess holds on legitimate customer deposits, leading Congress to prioritize prompt funds availability.[737] Advances in payment processing have largely eliminated those delays, but they have also enabled fraudsters to exploit accelerated access to funds before suspicious transactions can be fully investigated.

Today, Reg CC's rigid funds-availability framework can limit financial institution's ability to introduce risk-based "smart friction" when credible fraud indicators are present.[738] While Reg CC permits certain exception holds, those exceptions are narrowly defined and were not designed for the scale and sophistication of modern fraud schemes, including the risk of counterfeit Treasury checks, altered official checks, account takeover, and social engineering scams.[739] As described above, financial institutions are increasingly relying on machine learning, behavioral analytics, and consortium data to identify suspicious activity, yet Reg CC often requires funds be made available before these tools can complete meaningful verification.[740]

Treasury check fraud illustrates this challenge. Counterfeit and altered Treasury instruments have become a significant source of losses, often involving organized criminal networks.[741] Because Treasury checks are generally afforded expedited availability and carry an assumption of legitimacy, they remain attractive targets for fraudsters seeking to withdraw or transfer funds before verification can occur.[742]

More broadly, Reg CC reflects a policy framework developed when delayed access to legitimate funds posed the primary risk to consumers. Today, financial fraud increasingly exploits speed, immediacy, and irreversibility. As payments systems continue to accelerate, a regulatory structure that emphasizes prompt availability while providing limited flexibility for

---

[736] *Compliance Guide to Small Entities (A Guide to Regulation CC Compliance)*, BD. OF GOVERNORS OF THE FED. RSRV. SYS. (Dec. 12, 2025), https://www.federalreserve.gov/supervisionreg/guide-regulation-cc-compliance.htm.
[737] *Regulation CC (Availability of Funds and Collection of Checks)*, BD. OF GOVERNORS OF THE FED. RSRV. SYS. (May 17, 2024), https://www.federalreserve.gov/paymentsystems/regcc-about.htm.
[738] Letter from Am. Bankers Assoc., to Chief Counsel's Off., Off. of the Comptroller of the Currency, re: Docket ID Occ-2025-0009 – OCC Request for Information on Potential Actions to Address Payments Fraud (Sep. 18, 2025), *available at* https://www.aba.com/-/media/documents/comment-letter/clpaymentsfraud20250918.pdf?rev=65b45e30d1034b2191e313c83485658f.
[739] *Id.*
[740] FED. BUREAU OF INVESTIGATION, INTERNET CRIME REPORT 2023 (Apr. 4, 2024), *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf [hereinafter FBI 2023 INTERNET CRIME REPORT]; Mary Ellen Biery, *Reg CC new account hold: Funds availability & fraud risks*, ABRIGO (Feb. 29, 2024), https://www.abrigo.com/blog/reg-cc-funds-availability-requirements-and-fraud/.
[741] U.S. DEP'T OF THE TREASURY, 2024 NATIONAL MONEY LAUNDERING RISK ASSESSMENT 15-17 (2024), *available at* https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf; FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN. TREND ANALYSIS, MAIL THEFT-RELATED CHECK FRAUD: THREAT PATTERN & TREND INFORMATION, FEBRUARY TO AUGUST 2023 (2024), *available at* https://www.fincen.gov/system/files/shared/FTA-Check-Fraud-FINAL508.pdf.
[742] Mary Ellen Biery, *Treasury Check Verification System (TCVS): Preventing check fraud*, ABRIGO (Mar. 13, 2025), https://www.abrigo.com/blog/u-s-treasury-check-verification-fight-tax-season-fraud/.

risk-based verification hinders financial institutions' ability to prevent fraud and protect consumers. At the same time, regulators and Congress must be cognizant that delays in funds' availability may negatively impact consumers by limiting access to legitimate funds.

For these reasons, a large focus of the previously discussed RFI from the OCC, FDIC, and Federal Reserve was on considerations relating to Reg CC and whether its timelines for funds availability and exceptions framework provide sufficient flexibility to fight fraud. Commenters specifically focused on permitting exceptions for EFTs,[743] clarifying the reasonable cause to doubt collectability exception,[744] expanding the definition of new account to go beyond 30 days,[745] and generally modernizing Reg CC to better manage fraud and scams risks.[746]

H. Prioritizing Investigation and Prosecution of Fraudsters & Scammers

When a burglar breaks into someone's home and steals $300,000 worth of items, there is a presumption that the crime warrants a detective's attention, a prosecutor's time, and potentially a jury's verdict. When a criminal organization steals $300,000 from a retired schoolteacher through a months-long romance scam—emptying her savings and destroying her mental health—there is, in most cases, unfortunately, no investigation, no prosecution, and no consequence for the perpetrators whatsoever. Fraud has become the largest property crime in the country by dollar value, surpassing all other categories of theft combined.[747] It affects tens of millions of people every year. It destroys retirements, breaks up families, and drives some of its victims to suicide. And yet the criminal justice system treats it, in most cases, as an acceptable loss—a problem for banks, regulators, and self-help hotlines, not for detectives, prosecutors, and juries. As the Aspen Institute wrote:

> The United States has powerful, world-leading criminal investigation and prosecution capabilities, backed by a strong criminal law code. However, . . . scam criminals' speed often overcomes the slower, deliberate nature of law enforcement methods, and their sophisticated, well-funded technological capability is outpacing law enforcement's capacity to stop them. And because they operate from overseas safe havens, scam criminals are often beyond the reach of U.S. law enforcement, especially civil law enforcement agencies and their usual enforcement tactics,

---

743 Letter from National Consumer Law Center to Bd. of Governors of the Fed. Rsrv. Sys. (Sep. 15, 2025), https://www.nclc.org/wp-content/uploads/2025/09/2025.09.15_Comments_Fraud-RFI-on-Payments-Fraud.pdf.
744 Letter from Indep. Cmty. Bankers of Am., to Bd. of Governors of the Fed. Rsrv. Sys. (Sep. 18, 2025), https://www.icba.org/documents/45248/1180442/ICBALetterRespondingtoBankingAgenciesRFIonPaymentsFraud.pdf/79cc74ad-2c4c-a408-6dea-af142e963f9f?t=1773848742649.
745 Letter from Consumer Bankers Assoc. to Bd. of Governors of the Fed. Rsrv. Sys. (Sep. 18, 2025), https://consumerbankers.com/wp-content/uploads/2025/09/CBA-Comment-Request-for-Information-on-Potential-Actions-to-Address-Payments-Fraud-Docket-ID-OCC-2025-006-Docket-No-OP-1866-RIN-3064-ZA49-1.pdf.
746 Letter from Bank Pol'y Inst. to Bd. of Governors of the Fed. Rsrv. Sys. (Sep. 18, 2025), https://bpi.com/wp-content/uploads/2025/09/BPI-Response-to-RFI-on-Potential-Actions-to-Address-Payments-Fraud.pdf.
747 *Property stolen and recovered in the United States in 2023, by type and value*, STATISTA, https://www.statista.com/statistics/252440/property-stolen-and-recovered-in-the-us-by-type-and-value/?srsltid=AfmBOop9HSBR8OEZ70zVUSGlg1b9FdFcS0O-Vz8h27QYMs-0Ig1qNKSS (last visited June 29, 2026). *Cf.* FBI 2025 INTERNET CRIME REPORT, *supra* note 25, at 4.

which rely on domestic legal injunctions, fines, and the like. This leaves criminals undeterred and the American public vulnerable to exploitation.[748]

The result is a signal, broadcast clearly to every criminal organization on earth, that stealing from Americans through deception is essentially risk-free. In briefings with Committee staff, nearly all private industry stakeholders expressed that law enforcement needs to play a larger role in disrupting and prosecuting criminal networks behind financial fraud and scams. These stakeholders noted that until criminals believe there is a penalty for their crimes, nothing will change.[749] Ultimately criminals must understand that the risk of their actions outweighs any reward. Until that signal changes, no amount of consumer education, technical friction, or interagency task forces will be sufficient to reverse the trajectory of this crisis.

Various law enforcement entities play a role in investigating fraud and scams, including but not limited to, local law enforcement, state attorneys general, the U.S. Secret Service, the FBI, the DOJ broadly, FinCEN, and the U.S. Postal Investigation Service.[750] Although the variety of entities responsible for investigating fraud demonstrates the widespread and varied nature of fraud and scams, it also contributes to related issues described above, such as confusion among victims as to where to report and limited information sharing that is vital to combating fraud.[751]

The sheer volume of fraud reports requires law enforcement to prioritize the largest and most widespread cases of fraud. Moreover, given that the average reported loss in a fraud case is $500,[752] the cost of investigating and prosecuting a fraudster or scammer can quickly exceed its expected return. Despite recognizing the increasing complexity of the scam life cycle, the USAO D.C.—together with the DOJ and FBI staff more broadly—acknowledged that resource limitations exist.[753] According to officials, every U.S. attorney office has a different intake and threshold number, or loss amount, necessary to initiate an investigation and case.[754] The U.S. Attorney's Office for the District of Columbia, DOJ, and FBI staff contended that this threshold concept is necessary to maximize cases that will have the most significant impact.[755] Another stakeholder in the law enforcement space acknowledged that they must prioritize the "most deceptive and highest dollar loss" fraud and scams, although this stakeholder acknowledged that they do look for commonalities across reports, which could result in aggregating the dollars lost.[756] As a result, many victims' reports are not investigated, which may discourage victims

---

748 ASPEN INST., UNITED WE STAND, *supra* note 282, at 15-16.
749 Briefings with Committee Republican staff (notes on file with Committee).
750 *How We Can Help You, Do Yourself a Favor: Be Crime Smart*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/how-we-can-help-you/scams-and-safety (last visited June 29, 2026); *Fraud Section (FRD),* CRIM. DIV., U.S. DEP'T OF JUST., https://www.justice.gov/criminal/criminal-fraud (last visited June 29, 2026); *What We Do*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/about-fincen/what-we-do (last visited June 29, 2026); *Our Investigation Starts With Your Report*, U.S. POSTAL INVESTIGATION SERV., https://www.uspis.gov/report (last visited June 29, 2026); *Bureau of Consumer Protection*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection (last visited June 29, 2026); *Financial Investigations,* U.S. SECRET SERV., https://www.secretservice.gov/investigations/financial (last visited June 29, 2026).
751 ASPEN INST., UNITED WE STAND, *supra* note 282; GAO-15-49SP, *supra* note 699.
752 2024 FTC DATA BOOK, *supra* note 12.
753 Briefing with House of Representatives staff (notes on file with the Committee).
754 *Id.*
755 *Id.*
756 Briefings with Committee Republican staff (notes on file with the Committee).

from reporting. Several stakeholders suggested to Committee staff that it would be beneficial to improve opportunities for aggregating claims to meet the threshold required to initiate an investigation, particularly at the FBI and DOJ levels.[757]

As mentioned above, fraud schemes are increasingly cross-institutional, cross-platform, and often transnational.[758] Unfortunately, law enforcement authorities typically receive information only *after* a suspicious transaction has occurred and been reported.[759] Under the BSA, financial institutions must file SARs for potentially illicit activity, but SARs are retrospective and institution-specific. Law enforcement does not receive real-time, consolidated transaction data across institutions.[760] Instead, investigators often must piece together activity from multiple SARs filed by different banks, sometimes weeks or months after funds have moved. GAO has noted that law enforcement's ability to leverage BSA reporting depends heavily on data quality, timeliness, and interagency coordination, all of which present ongoing challenges.[761] Information-sharing mechanisms between financial institutions and law enforcement are also constrained by statutory privacy and confidentiality rules discussed above.[762] As a result, law enforcement typically relies on institution-initiated reports rather than proactive, sector-wide analytics that could identify linked accounts, mule networks, or rapid cross-rail fund transfers before funds dissipate.

The existing federal prosecutorial architecture has made genuine progress. The DOJ Fraud Section grew by over 30 percent in 2025, ending the year with over 200 prosecutors[763]—a particularly striking expansion given reductions elsewhere in the federal government. The National Fraud Enforcement Division, announced in January 2026, brings coordinated prosecutorial capacity across the DOJ for the first time. The Scam Center Strike Force has demonstrated that a targeted, well-resourced, interagency enforcement can produce results, with more than $700 million in seized digital assets, arrests of compound managers in Southeast Asia, and the first-ever seizure of a Telegram channel used for trafficking victims into fraud operations. These efforts must also be bolstered by a reorientation of enforcement priorities that reach beyond federal prosecutors to state attorneys general, local district attorneys, and the full range of law enforcement agencies that receive and file fraud complaints.

Such an expansion and reorientation also requires a shift in how law enforcement addresses these crimes.[764] Unfortunately, however, frontline officers and investigators are "experiencing fatigue, frustration, and burnout linked to the high volume of cybercrime cases

---

757 Briefings with Committee Republican staff (notes on file with the Committee).
758 *See* FBI 2023 INTERNET CRIME REPORT, *supra* note 740, at 5-8, 18-24 (describing cross-border and multi-institution fraud schemes involving rapid transfers through mule accounts).
759 *See* 31 U.S.C. § 5318(g)(1).
760 *See, e.g.*, BANK POL'Y INST., FRAUD AND SCAM PREVENTION PLAYBOOK (Feb. 4, 2026), https://bpi.com/fraud-and-scam-prevention-playbook/ (noting current fraud information sharing is "too reactive" and recommending legal safeguards to enable real-time collaboration).
761 *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-19-582, ANTI-MONEY LAUNDERING: OPPORTUNITIES EXIST TO INCREASE LAW ENFORCEMENT USE OF BANK SECRECY ACT REPORTS (2019).
762 *See id.*
763 FRAUD SECTION, CRIM. DIV., U.S. DEP'T OF JUST., 2025 YEAR IN REVIEW (2026), https://www.justice.gov/criminal/media/1425226/dl.
764 *See generally* FBI 2023 INTERNET CRIME REPORT, *supra* note 740.

and limited resources."[765] As a result, many local police departments face financial and personnel resource limitations.[766] These issues are also compounded by state and local law enforcement lacking the training needed to address increasingly complex and technical crimes, like fraud and scams. It is necessary that law enforcement entities receive specialized training in digital forensics, tracing, and the technical nature of internet-based crime. At least one company told Committee staff that they host regular summits with state and local law enforcement entities to teach the participants about trends and evolving technology.[767] However, these are informal, company-driven events. Ensuring that law enforcement has the training and resources they need to address fraud and scams requires a sustained, formal effort.

I. Continuing to Adapt & Utilize Technology

The fraud epidemic did not emerge from nowhere. It was, in substantial part, a product of technology, which has lowered the cost of impersonation, eliminated the geographic constraints of crime, automated the mechanics of deception, and placed professional-grade manipulation tools in the hands of anyone willing to pay for them. The deepfake that costs $25 million in a single fraudulent wire transfer, the AI voice clone that persuades a grandmother she is talking to her grandson in crisis, the phishing email indistinguishable from a bank's authentic communications—these are not feats of human cunning alone. They are feats of engineering, deployed at scale by criminal organizations that have embraced technological innovation as a core competitive strategy.

As many stakeholders refrained, "the only way to beat bad technology, is through good technology." As one witness testified before the Committee, "the solution to the criminal abuse of AI is not to ban or stifle the technology. It is to use it and use it wisely. We must stay a step ahead of illicit actors by leveraging the same innovations they use for harm for good."[768]

Every industry caught up in the fraud and scam lifecycle must embrace the same technological frontier that criminals are exploiting, deploying AI, machine learning, blockchain analytics, behavioral biometrics, and real-time data intelligence to fight at the same level of sophistication as the adversary. Current approaches include behavioral analytics, identity threat detection, network traffic analysis, AI-powered email security, deepfake detection tools, and evolved security awareness training platforms. AI, in particular, will be a core component for fraud teams as they face a new wave of sophisticated threats in the future. The public sector must follow the same logic. Regulatory agencies, law enforcement bodies, and government program administrators that rely on manual review processes, periodic audits, and static threshold-based detection systems are systemically slower and less accurate than the AI-powered fraud operations targeting them. As one stakeholder noted, while the technology used in in fraud and scams is

---

[765] Christopher J. Moloney et al., *Assessing Law Enforcement's Cybercrime Capacity and Capability*, FED. BUREAU OF INVESTIGATION (Apr. 6, 2022), https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability-.
[766] *Id.*
[767] Briefings with Committee Republican staff (notes on file with the Committee).
[768] *Modernizing the BSA for Financial Crimes in the 21st Century*, *supra* note 45 (statement of Ari Redbord, Global Head of Policy, TRM Labs).

ever changing, "the federal government is not the best at quickly adapting to the changing landscape."[769]

And the competitive dynamics require continuous investment rather than one-time deployment. Fraud detection systems are only effective for as long as criminal networks have not yet learned to evade them. Adversaries are constantly and actively studying deployed defensive systems and designing attacks to defeat them. This means that machine learning models trained on historical fraud patterns must be continuously retrained as new attack patterns emerge. Deepfake detection tools that identify artifacts specific to today's generation of synthesis technology must be updated as synthesis technology improves. Behavioral models that define normal account activity must be recalibrated as customer behavior evolves. Further, financial institutions must work to draw on all available sources of information within their control. As one stakeholder stated, "anti-money laundering efforts have become a compliance checklist;" banks should be looking not only at transaction data, and red flags, but also know-your-customer information to inform a wholistic picture.[770]

Further, all industries involved should be making protections available for consumers. As Mr. Paul Benda, Executive Vice President of Risk, Fraud, and Cybersecurity at the American Bankers Association, testified:

> By the time a victim is ready to send a payment, they often believe they know and trust the scammer. Caller ID might display the bank's name. A text message might look identical to a legitimate fraud alert. A social media ad might appear to come from a trusted company. These are tools banks do not control. That is why banks cannot fight this battle alone. Other stakeholders must step up. Telecommunications companies must stop criminals from impersonating banks through spoofed phone calls and fraudulent texts.[771]

This includes making preventative technology available at scale. For example, various tech companies informed Committee staff about protections they have introduced for customers—such as call screening features—yet these are made *opt-ins*, meaning that consumers must manually activate such protections.[772] Such protections could be made *opt-outs*, giving consumers the option to turn it off if they so choose.

Similarly, one stakeholder in the financial sector told Committee staff that at least one entity in the telecommunications space makes available technology through which the two companies can work together to block spoofed calls purporting to be the financial sector entity, but at a cost.[773] While the financial sector stakeholder had purchased this technology for the benefit of their customers, not all stakeholders have done the same. Additionally, as noted above, while telecommunications companies are making some protections available if the customer affirmatively chooses, at least one telecommunications company offers further protections to

---

769 Briefings with Committee Republican staff (notes on file with the Committee).
770 Briefings with Committee Republican staff (notes on file with the Committee).
771 *Fraud in Focus*, *supra* note 42 (statement of Mr. Paul Benda, Exec. Vice President of Risk, Fraud, and Cybersecurity, American Bankers Ass'n).
772 Briefings with Committee Republican staff (notes on file with the Committee).
773 Briefings with Committee Republican staff (notes on file with the Committee).

customers for an extra $4 per month.[774] Offering such technology and tools at scale would be a small step in better addressing these issues.

The above examples underscore how many companies outside of the financial sector are driven to address fraud and scams more by consumer incentives than by legal incentives. As explained above, financial institutions are legally responsible for reimbursing customers in the event of unauthorized payments; telecommunications and social media companies largely do not face that same burden. Certain stakeholders with whom Committee staff engaged argued that imposing similar legal responsibilities across other industries would do more to drive those companies to address issues on their platforms.[775] For example, many stakeholders noted that such liability was especially important in addressing fraudulent advertisements, since the host platform benefits financially from those posts.[776]

CONCLUSION

The fraud and scams epidemic is not a problem that will solve itself. It is one that is growing in scale, sophistication, and human cost, accelerating faster than the collective response of the United States government and industry. Thankfully, the tools, desire, and institutional capacity to fight back exist. Some private sector companies are investing heavily in protection. The Trump Administration has taken meaningful steps to elevate fraud and scams as a federal priority. Law enforcement—federal, state, and local—have demonstrated, through initiatives like the Scam Center Strike Force, that targeted and coordinated action produces real results.

However, good intentions and isolated efforts are not enough. What is required is a unified, sustained, whole-of-ecosystem commitment—a commitment that breaks down silos between industries, aligns government agencies around a common strategy, empowers consumers with consistent and coordinated education, and ensures that criminal networks understand that defrauding Americans carries real consequences. The barriers to effectively mitigate fraud and scams are not insurmountable, but they will not fall on their own, and the tens of millions of Americans victimized each year cannot afford to wait.

[774] *See Scam Sheild*, T-MOBILE, https://www.t-mobile.com/benefits/scam-shield (last visited June 29, 2026) (offering a premium version for an additional cost).
[775] Briefings with Committee Republican staff (notes on file with the Committee).
[776] Briefings with Committee Republican staff (notes on file with the Committee).