

Testimony for the Record
Submitted to the Joint Economic Committee
Hearing on
“The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from
Foreign Fraudsters”
March 25, 2026

Kate Griffin
Director, Inclusive Finance
The Aspen Institute Financial Security Program

Chairman Schweikert, Ranking Member Hassan, and distinguished members of the Joint Economic Committee,

Thank you for inviting me to testify today on an issue that is presenting a threat to our national security, to the systems of communication, commerce, and finance in our country, and to American households’ financial security: Scams - the ability of criminals to deploy sophisticated technological tools and psychological warfare to socially engineer everyday consumers into sending money and personal information.

The United States is caught in a global conflict with these scammers, and we are not yet winning. Working mostly from safe havens overseas, criminals are exploiting America’s communications, banking, and digital platforms to deceive Americans into sending money, divulging sensitive information, or worse. A majority of Americans say they get scam calls, emails, and texts at least weekly, and more than 50 million U.S. adults have lost money to an online scam or attack.¹ This causes American households to lose more than three billion dollars *every week*, among other harms. Often, scammers are part of transnational criminal organizations that use fraud and scams to fund other crimes, including drug and human trafficking. In addition to lowering criminals’ barriers to entry, cryptocurrency and artificial intelligence-powered deepfakes are fueling the scams boom, enabling ever-faster and more powerful forms of criminal deceit.

¹ Jeffrey Gottfried, Eugenie Park, and Monica Anderson, “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/>.

A ratio of 1 in 5 adults equates to approximately 53 million adults, based on a total U.S. adult population of approximately 267 million. See: U.S. Census Bureau, “National Population by Characteristics: 2020-2024,” June 2025. <https://www.census.gov/data/tables/time-series/demo/popest/2020s-national-detail.html>.

In 2024 and 2025, the Aspen Institute Financial Security Program (Aspen FSP) convened the **National Task Force for Fraud and Scam Prevention** to bring together stakeholders interested in stopping this crime, protecting consumers, and restoring trust in our systems. During that time, at least 300 experts from more than [80 organizations](#)—including some of the largest companies on the frontlines against scammers, such as JPMorgan Chase, Google, Target, Microsoft, Verizon, Amazon, and Meta- contributed thousands of hours to it. It was the first time such a broad collection of leaders from government, law enforcement, private industry, and civil society came together in the United States to help develop a whole-of-ecosystem strategy to prevent scams.

My testimony today reflects insights gained from the Task Force and key recommendations from the report titled ["United We Stand: A Strategy to Prevent Scams,"](#) which Aspen FSP released on October 1st, 2025.² The report calls for a national strategy to combat scams, focusing on prevention and public-private coordinated action. It recommends key policies and practices for each step of the scam lifecycle. It also includes dozens of practical steps that companies and government agencies could take to improve our scam defenses, and it identifies many promising innovations that are worth testing.

America must undermine the scams business model, making this criminal enterprise harder, riskier, and less profitable, as well as easier to detect and deter. Doing so will require deploying the best of the American spirit: bold leadership, innovative thinking, and well-coordinated effort.

But right now, the scams epidemic is a major threat to American prosperity and national security. We have attached a useful summary of the scale and impact of this epidemic (see Appendix I: Scam Threat Overview). Below is a handful of ***the most distressing facts about the scams threat in America:***

- **1 in 5 U.S. adults** (53 million) claim they lost money to an online scam or attack.³ Everyone is at risk of becoming a scam victim.⁴
- FBI and FTC complaints document about \$16 billion and \$12 billion in annual losses, respectively, and the FTC estimates that **actual fraud-related losses to U.S. consumers exceed \$196 billion per year.** (This is an increase from last year's

² Aspen Institute Financial Security Program. Nick Bourke, Erin Borg, Laila Bera, Molly Rubenstein, and Kate Griffin. "United WeStand: A National Strategy to Prevent Scams." Aspen Institute Financial Security Program, 2025. <https://fraudtaskforce.aspeninstitute.org/nationalstrategy>.

³ Gottfried, Park, and Anderson, "Online Scams and Attacks in America Today."

⁴ Ibid.

estimate of \$158 billion in annual losses.) This means that the scams industry now rivals the size of the illicit drug industry and is growing fast.⁵

- Being tricked by a scammer to send money or provide access to a financial account is the **second-largest crime concern** in the U.S. (second only to identity theft).⁶
- Bipartisan majorities of U.S. adults say the federal government is doing a **“bad job”** handling online scams and attacks.⁷

It's not *just* that criminals are stealing *billions* of dollars *every week* from American households. **It's also *how they're doing it*: by preying on people almost everywhere, including on their phones and other devices.** Most U.S. adults report receiving scam messages daily or weekly through phone (68%), email (63%), or text (61%), and 33% report the same through social media.⁸

Criminals are also rapidly adopting new technologies to increase the effectiveness and efficiency of their operations, making their business models even more profitable. For example, multilingual translation tools and LLMs are being leveraged to scale romance scams. These AI tools are being exploited by criminals to streamline their internal scam compound operations, including reducing the need for human oversight. These tools are also being used to optimize social engineering methods to appear more legitimate.⁹

⁵ The rise of online scams represents a substantial transfer of wealth from middle-class households to organized criminal networks. See, e.g., The Economist. "Online Scams May Already Be as Big a Scourge as Illegal Drugs." February 6, 2025. <https://www.economist.com/briefing/2025/02/06/online-scams-may-already-be-as-big-a-scourge-as-illegal-drugs>.

⁶ Gallup. "Scams Relatively Common, Anxiety-Inducing for Americans." July 31, 2023. <https://news.gallup.com/poll/544643/scams-relatively-common-anxiety-inducing-americans.aspx>.

⁷ Gottfried, Park, and Anderson, "Online Scams and Attacks in America Today."

⁸ Ibid.

⁹ TRM Labs. "AI-Enabled Fraud: How Scammers Are Exploiting Generative AI." May 7 2025.. <https://www.trmlabs.com/resources/blog/ai-enabled-fraud-how-scammers-are-exploiting-generative-ai>. According to the U.S.-China Economic and Security Review Commission generative AI is "turbocharging" scam operations through three specific technical tactics including, evading security filters, mass outreach and lowering technical barriers. Scammers use AI image generators to create unique social media profiles that bypass reverse image searches, which are typically used to identify stolen or reused photos. They use LLMs to "churn out" enormous quantities of initial contact messages and engage with large pools of victims simultaneously, allowing a single scammer to do the work that previously required an entire team. AI coding tools allow mid-level developers to create "scamming kits" that make SMS phishing campaigns automated, affordable, and highly scalable for lower-level criminals. For more information on AI enabled scam tactics see: U.S.-China Economic and Security Review Commission. "Protecting Americans from China-Linked Scam Centers: An Update on Emerging Trends." Published March 5, 2026. <https://www.uscc.gov/research/protecting-americans-china-linked-scam-centers-update-emerging-trends>

This is all made worse by the fact that trying to prevent and react to scam activity costs American companies—and by extension, their customers— billions of dollars more. Small businesses, which make up most U.S. firms, are facing constant, increasingly sophisticated cyberattacks. To cope with rising cybersecurity costs and the financial fallout of data breaches, nearly 40% are raising prices of their goods and services. This effectively creates a hidden “cyber tax” on consumers, who pay more while also suffering from data breaches and financial losses. The result is a drag on the U.S. economy that fuels inflation and hits resource-constrained small businesses hardest, forcing them to choose between security, growth, and affordable prices.¹⁰

This represents an affordability crisis that, for some reason, we haven’t been talking much about, and we’ve been *doing* even less. The scam epidemic is driving higher costs for consumers, lost savings, less prosperity, financial instability, and broken dreams.

And it’s not just money. This scam epidemic is eroding trust in America’s most important systems of commerce, communication, and government. The vectors of attack are varied, which is why we say this is an ecosystem problem. Scammers target victims on all the core systems of American commerce and communication: Telecoms, messaging, digital platforms (social media, paid advertising, retail), and financial services (banking, payments, fintech, crypto).

This reduces American economic well-being to a degree almost unrivaled, and it represents a major blow to the economic opportunity vision at the core of [this Committee’s mission](#).

This Committee cannot fix the scam problem alone, but it could play an important role in prioritizing and coordinating Congressional reforms to improve scam prevention in America.

Here’s how. Online scams are a *business* conducted by *sophisticated networks* that often benefit *pariah states* or *transnational criminal organizations* and their *corrupt enablers* (see Appendix I: Scam Threat Overview). The way to defeat “Scams, Inc.” is through a coordinated public-private effort to *undermine its business model*. This means making it harder, riskier, and less profitable to prey on Americans and the online systems they rely on:

- **Harder:** Help companies coordinate with each other, law enforcement, and diplomatic channels to improve their ability to deter, detect, and disrupt scam activity.

¹⁰ Identity Theft Resource Center. *2025 Business Impact Report: Small Business Cybersecurity in the Era of AI*. December 2025. <https://www.idtheftcenter.org/wp-content/uploads/2025/11/ITRC-2025-Business-Impact-Report.pdf>.

- Riskier: Improve the ability of law enforcement and diplomatic channels to pursue and punish scam criminals. This includes enhancing law enforcement’s powers to seize and force forfeiture of scam proceeds and dismantle scam compounds.¹¹
- Less Profitable: A coordinated, public-private national strategy to combat scams will improve our defenses, strengthen our collective ability to intervene and disrupt in real time, and make us better at punishing scam criminals and taking back their stolen funds. It will become more costly and less rewarding to be a scammer, and the scam business model will fade.¹²

The federal government, both Congress and the Executive Branch, must take bold action to meet this challenge and partner with private-sector companies that are on the front lines of the scam epidemic.

There is some good news:

We’ve learned a lot about what needs to be done. Companies have been experimenting and innovating. Examples from other countries, like Australia, have been instructive. As mentioned above, the Aspen FSP-led national task force on fraud and scam prevention brought together over 80 public and private sector organizations between 2024 and 2025, which informed the publication of the “[United We Stand](#)” report containing dozens of recommendations and scores of insights and practical ideas for both government and companies. Some of it is already happening naturally in the market. *Much of it will not happen unless Congress and the Executive Branch take coordinated action to empower it.*

Companies are acting. Companies are truly awake to the scams threat and have started investing heavily to combat it. This is good news. *They cannot succeed alone,* and their capabilities will remain severely constrained and disjointed unless policymakers help them, but

¹¹ As enforcement pressure increases in one jurisdiction, networks rapidly relocate and rebuild in new political and financial environments. This is evident by the resurgence of scam infrastructure and flight of scam operators from Cambodia and Myanmar into Vietnam, Laos, Malaysia, Dubai, Sri Lanka, and Indonesia, following the arrest of the Cambodian syndicate leader Chen Zhi, founder of the [Prince Group Transnational Criminal Organization](#). Therefore, more needs to be done to undermine the scam business model across the scam lifecycle. For information on the resurgence of scam infrastructure see: National Democratic Institute (NDI), Scam Brief: Tracking the Online Chinese-Language Scam Ecosystem, March 2026.

¹² In Southeast Asia, scamming has become a profitable domestic industry in states that harbor scam compounds. For example, the [Cambodian](#) scam industry generates between \$12.5 to \$19 billion per year, equivalent to as much as 60 percent of the country’s formal GDP. For information on South East Asia Scam Compounds see: Jacob Sims, *Policies and Patterns: State-Abetted Transnational Crime in Cambodia as a Global Security Threat*. Human Research Consultancy. May 2025. https://cdn.prod.website-files.com/662f5d242a3e7860ebcfde4f/68264cff356caba111f2db1e_Policies%20and%20Patterns_16052025.pdf.

they are trying, and they are becoming more coordinated. For example, the *Industry Accords Against Online Scams & Fraud* are a set of voluntary commitments by major global technology companies to work together to implement robust measures that protect consumers and combat scams perpetrated on their platforms.¹³ The American Bankers Association has expanded its Fraud Contact Directory program to include international banks in an unprecedented cross-border collaboration to stop fraudulent transactions as quickly as possible.¹⁴ Dozens of other companies have made pledges and commitments at the recent UN Global Fraud Summit.¹⁵

And while we see cutting-edge technology being used by the criminals, it's also a powerful tool in the fight: according to OpenAI, its models are used to detect scams up to three times more often than they are exploited by criminals to facilitate them. Users frequently prompt the model to help them identify potential scams, and it, in turn, flags suspicious activity and advises users on appropriate safety measures.¹⁶ This has led to its partnership with the Global Anti-Scam Alliance to build "Scam.org," a consumer-facing tool for identifying potential scams.¹⁷

The White House is acting. [Executive Order 14390](#) (March 6, 2026) directs the Attorney General and the Secretaries of State, Treasury, War, and Homeland Security to assess current authorities and identify gaps in federal capabilities to prevent cybercrime, financial fraud, and online scams. And importantly, it requires these agencies to *deliver an action plan to the President this summer*, working in conjunction with a senior White House advisor and the Office of the National Cyber Director. In doing so, the Executive Order appears to elevate scam prevention from a fragmented set of enforcement and regulatory activities to a whole-of-

¹³ Google. *Industry Accords Against Online Scams and Fraud*. 2026.

<https://services.google.com/fh/files/newsletters/industryaccord.pdf>.

¹⁴ American Bankers Association, "ABA Opens Fraud Contact Directory to International Banks, Expanding Global Effort to Combat Financial Crime." press release, March 17, 2026. <https://www.aba.com/about-us/press-room/press-releases/check-fraud-directory-expansion>.

¹⁵ For a full list of Global Pledge Signatories see: United Nations Office on Drugs and Crime. "Global Fraud Summit 2026 | Pledges." Accessed March 17, 2026. <https://www.unodc.org/unodc/organized-crime/global-fraud-summit/pledges.html>.

¹⁶ OpenAI. "Disrupting Malicious Uses of Our Models." February 25, 2025. <https://cdn.openai.com/threat-intelligence-reports/7d662b68-952f-4dfd-a2f2-fe55b041cc4a/disrupting-malicious-uses-of-ai-october-2025.pdf>.

¹⁷ Global Anti-Scam Alliance. "Global Anti-Scam Alliance Launches Scam.org with OpenAI and Key Partners." March 12, 2026. <https://gasa.org/knowledge-base/blog/global-anti-scam-alliance-launches-scam.org-with-openai-and-key-partners>.

government priority. Aspen FSP [summarized the EO and what the White House action plan should say](#), in a blog post dated March 10.¹⁸

Federal Agencies are acting. The [Scam Center Strike Force](#) is an example of an ongoing multi-agency initiative (DOJ, FBI, Secret Service, State Department, and Treasury) launched in 2025 that is directed by the U.S. Attorney's Office to dismantle Southeast Asian cryptocurrency fraud networks, seize illicit assets, and return stolen funds to victims. This is on the heels of multiple sanctions issued by the State and Treasury Departments in recent months.¹⁹

Congress is acting, too. A number of scam-related bills have been introduced in several committees, which shows that Congress has taken note of the need. Coordinating, prioritizing, and streamlining legislative action across all sectors of the digital economy will be an important next step. The latest appropriations process suggests a move in that direction, by including an agreement with the Department of Treasury to coordinate with a number of agencies and, by this Summer, submit a national strategy or plan to Congress that “leverages and augments local, State, and Federal resources within the financial sector to mitigate and prevent online scams.”²⁰ Further action to coordinate rules and practices across financial services and the other key industries, especially digital and social media platforms and telcos, should surely follow.

Congress should not wait to play its part in solving the scam problem. It would be a mistake for Congress to wait for the White House to publish a plan or for agencies to submit their reports. Rather, Congress should supplement and amplify these efforts and provide more resources for prosecution and sanctions against scammers.

If successful, the White House plan will launch a variety of coordinated, cross-agency activities; identify key gaps in the capabilities and information sources of law enforcement, intelligence, and financial oversight; establish an ongoing executive mechanism to coordinate agency actions, including law enforcement and diplomatic interventions; and promote better

¹⁸ Nick Bourke and Kate Griffin. “The White House Acts on Scams: What Comes Next.” *Aspen Institute* (blog). March 10, 2026. <https://www.aspeninstitute.org/blog-posts/the-white-house-acts-on-scams-what-comes-next/>.

¹⁹ U.S. Department of the Treasury's Office of Foreign Assets Control has imposed sanctions state & non-state sponsored TCOs for scam related activity, including [Southeast Asian Networks](#) operating in Shwe Kokko, Burma, a notorious hub for virtual currency investment scams under the operational control of the [OFAC-designated Karen National Army \(KNA\)](#), [The Zhao Wei Transnational Criminal Organization](#) operating in the illusive scam compound at the border of Myanmar, Laos, and Thailand, also known as [The Golden Triangle Special Economic Zone](#), [The Lazarus Group](#), which has ties to the North Korean government, channels revenues generated from fraud and scams to the regime, and [The Jalisco New Generation Cartel](#) runs scam call centers that finance narcotics trafficking and money laundering.

²⁰ U.S. Congress, Congressional Record, House, January 14, 2026, p. H812. <https://www.congress.gov/119/crec/2026/01/14/172/10/CREC-2026-01-14.pdf>.

coordination and information sharing with the private sector companies that operate the platforms scammers target: digital and social media platforms, telecommunications companies, and financial and payments firms.

But the White House review will surely highlight a number of needs that only Congress can help fix, creating an opportunity for Congress to be at that table and preparing for action. For example, it will be necessary to amend the laws to adequately improve law enforcement's powers to seize and force forfeiture of digital and other assets that scammers steal. Congress should pay attention to and designate senior leadership staff to engage with the White House process. At a minimum, this would create valuable opportunities for Congressional leaders to learn and strengthen relationships with experts across the ecosystem; and it will probably generate very clear ideas for bills that Congress should be preparing now, and critically, how to prioritize them as part of empowering America's scam prevention strategy. This is true not just for this committee, but at a leadership level that coordinates Congressional action across committee and industry silos.

Five things that Congress should do now:

First and foremost, form a plan and prioritize legislative reforms. Scams are a whole-of-economy threat, perpetrated across all the relevant industries—digital platforms, telcos, banks, and payments firms. The solution must be a whole-of-economy solution that coordinates interventions and information sharing across these industry and Congressional committee silos. Like the federal agency process initiated by EO 14390, Congress could launch a cross-committee, whole-of-Congress process to (1) review needs and shortfalls; and (2) prioritize and implement reforms. Again, this can and should be done concurrently with—and learning from—the federal agency process that is now underway.

Next, act on three important scam prevention goals. Available evidence suggests that the following three priorities are among the most urgent legislative needs for undermining the scams business model. These are summarized below and described in detail in the [“United We Stand”](#) report, along with many practical suggestions. (Page references below cite the downloadable PDF of the report.)

- **Enhance law enforcement's powers to seize or achieve forfeiture of criminals' digital assets and restore funds to victims.** (pp. 15-19; 38-41.)
- **Clarify the duties that companies have to protect customers from online scams, harmonize them across the ecosystem, and provide sufficient legal safe harbors to empower companies to pursue those duties.** This should include facilitating the sharing of actionable scam intelligence among each other and relevant government

agencies, and acting on that information. (These ideas are discussed throughout the “*United We Stand*” report; see, e.g., pp. 51-54; 26-29; and 30-32.)

- **Commit resources to make key federal criminal reporting and analysis systems fit-for-purpose.** (pp. 32-37; and 50-51.)

Finally, act opportunistically on “low-hanging fruit” reforms to help victims and improve scam prevention. Though coordination and prioritization is important for obtaining real results, Congress need not wait for a perfect, comprehensive system. Aspen FSP’s “*United We Stand*” report offers dozens of near-term solutions, often found in the “*Practical Next Steps and Possible Solutions*” subsection at the end of each section. These include:

- Direct the study or creation of a “national front door” for scam reporting, with standardized intake and routing for existing law enforcement databases (FBI IC3, FTC Sentinel, FinCEN SARS). (pp. 32-34.) This should include consideration for bulk or aggregated reporting by the private sector in addition to consumers, as most victims do not report directly to law enforcement, but the vast majority tell their financial institution.²¹
- As needed, clarify laws or direct the establishment of harmonized regulatory guidelines or safe harbors for companies to flag actors and activities and pause, slow down, or reject payments or other transactions, where warranted by actionable scam intelligence. (e.g., p. 32 and footnote 62.)
- Direct or test the implementation of government-wide scam measurement and tracking, such as what the GAO has recommended, and require government agencies to report scam activity and trends for industry and public use on a regular basis. (p. 44.)
- Improve law enforcement training programs for officers and prosecutors, focused on improving ability to recognize scam activity and how to react effectively when it is detected or reported. This should include more standardized training programs for

²¹ Victims rarely report financial fraud to law enforcement. Among victims who lost money to scams or online attacks, 3 out of 4 U.S. adults report fraud or scams directly to their primary financial institution, while about 1 in 12 U.S. adults report to the police or law enforcement. Among those who reported to an institution, 14 percent reported that they were made to feel blamed or personally responsible. Although fraud and scams affect all Americans, some populations are more likely to feel blamed when seeking help than others. Victims also cite confusing procedures, shame, and hopelessness as reasons for not seeking help from authorities. For more information on victim reporting and blame see: Laila Bera, Shehryar Nabi, “A Pervasive Threat: Analyzing Recent Survey Data on Fraud and Scams.” https://www.aspeninstitute.org/wp-content/uploads/2025/12/2025_Fraud-and-Scams-Analysis_Report_FINAL.pdf.

state and local officials and, potentially, forming targeted federal-state collaborations or task forces to promote best practices and effective communication with the public. (pp.16-17.)

- Consider ways to promote robust private sector participation in anti-scam detection efforts, such as allocating incentives or promoting standards for safe and effective cross-sector corporate information exchange.(p. 29.)²²
- Provide relief to victims by eliminating or reducing tax penalties on early withdrawal of 401(k) funds sent to a scammer. (p. 41.)

Conclusion: A Call to Respond

Scams networks are sophisticated, often organized by Transnational Criminal Organizations, and are a pillar of the global criminal economy. Scam losses mean fewer dollars in the pockets of Americans, threatening households' financial security and long-term wealth-building ambitions. With targeted legislative action and a coordinated national strategy, Congress can help disrupt the scam business model and restore trust in the systems that underpin American prosperity and security.

Companies and government agencies are expending extraordinary effort to fight scams against consumers. They have had some success, and the recommendations in *“United We Stand: A National Strategy to Prevent Scams”* reflect lessons they have learned. But more is needed. The scams threat continues to grow as large volumes of criminals use rapidly evolving tactics to challenge the limits of our systems.

A ***whole-of-ecosystem*** response is urgently needed to undermine the criminal scam business model across the entire scam lifecycle, strengthen systems, and protect consumers.

The national response must emphasize collaboration between the government and the private sector.

- **Corporate leaders** must act decisively to suppress scam activity at every stage of its lifecycle. They must empower staff with resources and guidance to maintain robust

²² No single private-sector information-sharing exchange or industry possesses all the data, highlighting the need for cross-sector collaboration. The ultimate goal is to use this intelligence to take down the accounts and services scammers utilize, thereby making it more difficult for them to reach potential victims and eroding the profitability of the scam business model. For more information on the private sector information sharing landscape see: Laila Bera, and Molly Rubenstein. "Scaling Scam Prevention Through Shared Intelligence: Mapping the Solutions Landscape." Aspen Institute Financial Security Program. 2025. <https://fraudtaskforce.aspeninstitute.org/mapping-scam-solutions>.

anti-scam policies and respond effectively when scams occur. Companies in sectors targeted by scammers must keep up the fight.

- **Policymakers** must act boldly to enable the required response. Now that the **White House** has recognized scams as a national security threat and priority, **Congress** must empower a comprehensive private-sector response by enhancing incentives and modernizing legal frameworks, and it must drive better law enforcement and intelligence outcomes by tasking top officials with clear anti-scam goals, backed by sufficient funding and cross-jurisdictional authority.

These and other recommendations are further explained in Aspen FSP's report, titled "*United We Stand: A National Strategy to Prevent Scams.*" It presents extensive recommendations for government and private sector collaboration to combat fraud against consumers, cut off criminal funding, and protect the United States. Aspen FSP published the report in October 2025. We would be happy to brief Committee members and staff about the report or related issues.

For the full report and recommendations, see:
<https://fraudtaskforce.aspeninstitute.org/nationalstrategy>.

Appendix I: Overview of the Scams Threat

Scams threaten the livelihoods of all Americans

- 1 in 5 U.S. adults (53 million) claim they lost money to an online scam or attack.²³
- Everyone is at risk of becoming a scam victim.²⁴ Younger adults report experiencing scams in their households more than older adults, while older adults report losing about twice as much money when they are scammed.²⁵
- Scam victims are often revictimized. More than 1 in 10 U.S. adults (10.6 percent) had experienced multiple scams in the past year.²⁶
- FBI and FTC complaints document about \$16 billion and \$12 billion in annual losses, respectively, and the FTC estimates that actual fraud-related losses to U.S. consumers, accounting for under-reporting, exceed \$196 billion per year.²⁷

²³ Gottfried, Park, and Anderson, “Online Scams and Attacks in America Today.”

A ratio of 1 in 5 adults equates to approximately 53 million adults, based on a total U.S. adult population of approximately 267 million. See: U.S. Census Bureau, “National Population by Characteristics: 2020-2024,” June 2025. <https://www.census.gov/data/tables/time-series/demo/popest/2020s-national-detail.html>.

²⁴ National Consumers League. “Top Ten Scams of 2024.” January 16, 2025. <https://nclnet.org/wp-content/uploads/2025/01/Top-Scams-of-2024.pdf>.

²⁵ Younger households report experiencing scams at higher rates compared to older adults. According to a Gallup poll conducted in 2023, 22% of adults under 30 reported that someone in their household had fallen victim to a scam in the past year. This is notably higher than the 9% reported by those aged 50–64 and the 13% by those aged 65 and older. See, e.g., Gallup. “Scams Relatively Common, Anxiety-Inducing for Americans.” July 31, 2023. <https://news.gallup.com/poll/544643/scams-relatively-common-anxiety-inducing-americans.aspx>.

Seniors reported \$1.18 billion in fraud losses, compared to \$810 million reported by adults in their 30s. Despite the higher financial losses among seniors, the number of fraud reports from both age groups was similar, indicating that seniors are losing approximately 50% more per incident than their younger counterparts. See, e.g., U.S. Federal Trade Commission. “Consumer Sentinel Network Data Book 2024.”

²⁶ Laila Bera, Shehryar Nabi, “A Pervasive Threat: Analyzing Recent Survey Data on Fraud and Scams.”

²⁷ The 2024 Internet Crime Report combines information from 859,532 complaints of suspected internet crime and details reported losses exceeding \$16 billion—a 33% increase in losses from 2023. See: Federal Bureau of Investigation. “Internet Crime Report 2024.” Internet Crime Complaint Center (IC3). April 24, 2025. <https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>. Of the 2.6 million fraud reports, 38% indicated money was lost. In 2024, people reported losing over \$12 billion to fraud—an increase of over \$2 billion over 2023.

See: Federal Trade Commission. “Sentinel Network Data Book 2024.” March 2025.

<https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024>.

Federal Trade Commission. “Sentinel Network Data Book 2024.” March 2025.

<https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024>.

Federal Trade Commission. December 1, 2025. “Protecting Older Consumers 2024—2025.”

<https://www.ftc.gov/reports/protecting-older-consumers-2024-2025-report-federal-trade-commission>.

- Research suggests that the scams industry now rivals the size of the illicit drug trade and is growing fast.²⁸ Scam losses reported to law enforcement have more than tripled since 2019.²⁹

Text, phone, email, social media, and financial systems in America are at risk

- Most U.S. adults report receiving scam messages daily or weekly through phone (68%), email (63%), or text (61%), and 33% report the same through social media.³⁰
- 6 in 10 Americans or more say online scams are a “major problem” on text and phone, email, and social media, while roughly half say the same about shopping, banking, and payment sites or apps.³¹
- Being tricked by a scammer to send money or provide access to a financial account is the second-largest crime concern in the U.S. (57% of adults worry about it).³²
- Bipartisan majorities of U.S. adults say the federal government is doing a “bad job” handling online scams and attacks.³³
- Victims rarely report financial fraud to law enforcement. Among victims who lost money to scams or online attacks, 3 out of 4 U.S. adults report fraud or scams directly to their primary financial institution, while about 1 in 12 U.S. adults report to the police or law enforcement. Among those who reported to an institution, 14 percent reported that they were made to feel blamed or personally responsible. Although fraud and scams affect all Americans, some populations are more likely to feel blamed when seeking help

²⁸ The rise of online scams represents a substantial transfer of wealth from middle-class households to organized criminal networks. See, e.g., The Economist. “Online Scams May Already Be as Big a Scourge as Illegal Drugs.” February 6, 2025. <https://www.economist.com/briefing/2025/02/06/online-scams-may-already-be-as-big-a-scourge-as-illegal-drugs>.

²⁹ Reported scams in the U.S. rose between 2020 and 2024, with consumer complaints increasing from 4.7 million to 6.5 million and fraud losses growing from \$3.3 billion to \$12.5 billion (see, e.g., Federal Trade Commission 2020; 2024). U.S. Federal Trade Commission. “Consumer Sentinel Network Data Book 2020.” Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf.
U.S. Federal Trade Commission. “Consumer Sentinel Network Data Book 2024.” Federal Trade Commission. https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf.

³⁰ Gottfried, Park, and Anderson, “Online Scams and Attacks in America Today.”

³¹ Ibid.

³² Gallup. “Scams: Relatively Common and Anxiety-Inducing for Americans.”

³³ Gottfried, Park, and Anderson, “Online Scams and Attacks in America Today.”

than others.³⁴ Victims also cite confusing procedures, shame, and hopelessness as reasons for not seeking help from authorities.³⁵

Scams are a national security threat and a national priority

- The Annual Threat Assessment of the U.S. Intelligence Community has identified scams as part of a nexus of “criminal activity threatening the United States” perpetrated by Transnational Criminal Organizations (TCOs) and state-affiliated groups that also engage in human trafficking, drug trafficking, and weapons and human smuggling.³⁶
- North Korean hackers, Mexican cartels, Russian crime syndicates, and Triad gangs are among the U.S. adversaries that benefit from scams and other financial crimes.³⁷
- U.S. Department of the Treasury’s Office of Foreign Assets Control has imposed sanctions state & non-state sponsored TCOs for scam related activity, including [Southeast Asian Networks](#) operating in Shwe Kokko, Burma, a notorious hub for virtual currency investment scams under the operational control of the [OFAC-designated Karen National Army \(KNA\)](#), [The Zhao Wei Transnational Criminal Organization](#) operating in the illusive scam compound at the border of Myanmar, Laos, and Thailand, also known as [The Golden Triangle Special Economic Zone](#), [The Lazarus Group](#), which has ties to the North Korean government, channels revenues generated from fraud and scams to the

³⁴ Laila Bera, Shehryar Nabi, "A Pervasive Threat: Analyzing Recent Survey Data on Fraud and Scams."

³⁵ Many fraud victims do not report their crimes due to feelings of shame, guilt, or embarrassment, doubts about their own judgment, fear of others’ reactions, or belief that their losses are too small or that law enforcement will not act. Victims often blame themselves, even though skilled perpetrators are responsible.

See, e.g., U.S. Department of Justice, Western District of Washington. “Financial Fraud Crime Victims.” January 30, 2025. <https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud>.

Victim-blaming culture aimed at financial fraud victims, exacerbates victims’ deep sense of shame and low self-esteem and shifts the focus away from perpetrators.

See, e.g., AARP Fraud Watch Network and FINRA Investor Education Foundation, in collaboration with Heart + Mind Strategies. “Blame and Shame in the Context of Financial Fraud: A Movement to Change Our Societal Response to a Rampant and Growing Crime.” June 2022.

<https://www.finrafoundation.org/sites/finrafoundation/files/Blame-and-Shame-in-the-Context-of-Financial-Fraud.pdf>.

³⁶ Office of the Director of National Intelligence. “Annual Threat Assessment of the U.S. Intelligence Community.” March 2025. <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf>.

³⁷ TRM Labs. “All Roads Lead to China: North Korean Hackers, Fentanyl, Cartel Money Laundering, and Global Organized Crime.” May 27, 2025. <https://www.trmlabs.com/resources/reports/all-roads-lead-to-china>. See also: Ken Westbrook, “As Scams by Foreign Organized Crime Soar, Here’s How America Must Respond” (Stop Scams Alliance, December 2024), accessed September 3, 2025, PDF, 4-5. <https://static1.squarespace.com/static/6519507e53de4c0b643869f6/t/6758df9f5379a122c4f46952/1733877665261/As+Scams+by+Foreign+Organized+Crime+Soar%2C+Here%E2%80%99s+How+America+Must+Respond+.pdf>

regime, and [The Jalisco New Generation Cartel](#) runs scam call centers that finance narcotics trafficking and money laundering.

- Scam operations, which are often reliant on [forced human labor](#), are increasingly adopting technology to enhance their effectiveness and efficiency. The scam threat is rapidly evolving, and technological innovation provides criminal actors with opportunities to perpetrate new variations of low-risk, low-effort, high-profit business models. The FBI warned that criminals are increasingly exploiting artificial intelligence to create more convincing scams with less effort, using AI-generated images, audio, and video to impersonate trusted sources and deceive victims at scale.³⁸
- While these law enforcement efforts are promising, the regional scam economy is not collapsing - it is adapting. In Southeast Asia, scamming has become a profitable domestic industry in states that harbor scam compounds. For example, the [Cambodian](#) scam industry generates between \$12.5 to \$19 billion per year, equivalent to as much as 60 percent of the country's formal GDP. As enforcement pressure increases in one jurisdiction, networks rapidly relocate and rebuild in new political and financial environments. This is evident by the resurgence of scam infrastructure and flight of scam operators from Cambodia and Myanmar into Vietnam, Laos, Malaysia, Dubai, Sri Lanka, and Indonesia, following the arrest of the Cambodian syndicate leader Chen Zhi, founder of the [Prince Group Transnational Criminal Organization](#). Therefore, more needs to be done to undermine the scam business model across the scam lifecycle.³⁹

For the scam threat factsheet, see:

https://static1.squarespace.com/static/671a80aa4a84f2359ce4d360/t/6916172003e2b778e3ec19b4/1763058741494/AspenFSP-2405_Digital_Figure1_Final.pdf.

³⁸ FBI Internet Crime Complaint Center (IC3), "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud," Alert No. I-120324-PSA, December 3, 2024, <https://www.ic3.gov/PSA/2024/PSA241203>.

³⁹ National Democratic Institute (NDI), Scam Brief: Tracking the Online Chinese-Language Scam Ecosystem, March 2026.

Appendix II: “United We Stand: A National Strategy to Prevent Scams”

Below is a summary of recommendations highlighted in the report titled “[United We Stand: A National Strategy to Prevent Scams](#),” which presents recommendations for government and private sector collaboration to combat fraud against consumers, cut off criminal funding, and protect the United States. Aspen FSP published the report in October 2025.

Corporate Recommendations

Companies in sectors targeted or exploited by scammers, including telecommunications, messaging, digital platforms (social media, paid advertising, and retail), and financial services (banking, fintech, payments, and crypto) should:

- **Maintain robust anti-scam policies addressing the entire scam lifecycle.** C-suite level leaders should own these policies and include accountability mechanisms, adequate budget allocations, and clear expectations for customer service and data protection.
- **Strengthen system defenses.** Improve identity verification and authentication to block inauthentic actors, including evaluating the trustworthiness of advertisers and merchants. Use technology such as liveness testing and interoperable digital credentials to disrupt non-authentic communications.
- **Enhance capabilities to detect suspicious activity.** Invest in private information exchanges with companies in other sectors. Help improve standards for interoperability and ethical governance. Direct legal counsel to establish suitable compliance policies or seek necessary regulatory guidance or safe harbors.
- **Disrupt scams in process.** Take reasonable steps against suspicious activity based on actionable scam intelligence. Take down fraudulent communications channels (e.g. websites), deactivate accounts and profiles of bad actors, and dismantle scammer infrastructure. Continuously improve just-in-time warnings and interventions for customers.
- **Improve reporting and recovery mechanisms.** Share more actionable scam intelligence with law enforcement agencies. Promote effective recovery for victims by providing user-friendly reporting and dispute resolution mechanisms and ensuring fast correction of false positives or account takeovers (ATO).

- **Measure and evaluate interventions.** Pilot the proposed metrics framework for scams and report on results.⁴⁰
- **Collaborate with peers to strengthen scam defenses.** Share best practices across relevant industry sectors and advocate for policy improvements.

Public Policy and Government

The federal government and law enforcement and intelligence agencies, alongside state counterparts, should:

- **Elevate scam prevention as a national priority.** Starting with the White House and Congress, recognize scams as a national security threat and make scam prevention a whole-of-government priority. Establish a national strategy to combat scams, with dedicated resources and broad coordination mechanisms, such as a Congressional Commission or an administrative czar or division with whole-of-government authority. Empower and direct law enforcement and intelligence agencies to improve scam prevention outcomes.
- **Enhance incentives and modernize legal frameworks for combating scams.** Clarify duties for companies to prevent scam activity and de-risk participation in scam suppression efforts, by enacting “good Samaritan” liability protections for companies acting reasonably and in good faith.
- **Enhance law enforcement capabilities.** Increase statutory powers for asset seizure and recovery across all forms of money movement (including digital assets) and punishing transnational illicit financial activity. Create specialist anti-scam units, allocate resources, and develop training programs to improve recognition of scam activity and respond to it.
- **Combat cross-border financial crime.** Apply sanctions and use diplomatic tools against foreign governments and private parties that enable or benefit from scams. Formalize diplomatic engagements with allied nations to shut down scam centers. Improve intelligence gathering to disrupt transnational scam activity.
- **Modernize data collection and analysis.** Review and upgrade key law enforcement databases to improve data intake, analysis, and interoperability, leveraging modern technology like APIs and artificial intelligence (starting with FBI’s Internet Crime Complaint Center (IC3), FTC Sentinel, and FinCEN’s Suspicious Activity Reports (SARs) systems). Create a single portal (e.g. stopscams.gov) for companies to report scam intelligence, including mechanically or in bulk, with the system distributing inputs to the

⁴⁰ “Fraud and Scam Measurement Framework”. Aspen Institute National Task Force on Fraud and Scam Prevention. https://static1.squarespace.com/static/671a80aa4a84f2359ce4d360/t/6830b13e294cb446da01973d/1748021566525/MeasurementFramework_5-23-25.pdf.

appropriate government databases. Enhance law enforcement analytical capabilities to identify trends and improve deconfliction across agencies.

- **Improve feedback loops.** Law enforcement agencies should publish regular analysis of scam trends and prosecutions to industry and the public.
- **Implement recommendations from the U.S. Government Accountability Office (GAO).** Standardize measurement across agencies and develop a single, government-wide estimate of affected consumers and dollar losses, factoring in underreporting.⁴¹

Reforms Specific to Financial Services Policy

As part of a national strategy to combat scams, Aspen FSP’s national strategy details several reforms specifically relating to financial services, including:

- **Enhance information sharing efforts** to improve availability of actionable scam intelligence, by re-architecting the FinCEN SARS database to enable higher-volume and more automated data exchange and improving linkages with similarly revitalized FBI IC3 and FTC Sentinel databases.
- **Clarify or expand legal safe harbors** enabling financial institutions and non-financial institutions to exchange actionable scam intelligence and collaborate to prevent scams.
- **Establish parity of law enforcement powers across money movement**, including civil forfeiture of digital assets.
- **Enable risk-based payment pauses / limits** and other reasonable interventions to disrupt suspected malicious interactions.
- **Pilot bank-to-law enforcement victim report sharing.** Research shows that the vast majority of scam victims report the problem to their bank, while only a small portion report directly to a local or federal law enforcement agency.

Across the Ecosystem

All stakeholders should take a risk-based approach to flexibly prioritize interventions against the most impactful, and evolving, scam activities. Broader initiatives and cross-sector efforts should include:

- **Foster offensive technological innovation.** Use of artificial intelligence and advanced analytics is likely to be crucial for enhancing private and public sector capabilities in scam detection, prevention, and response.
- **Strengthen public awareness and consumer empowerment.** Study and improve consumer education, warning, and intervention practices. Increase funding for targeted,

⁴¹ “Consumer Protection: Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams” Government Accountability Office, April 8, 2025. <https://www.gao.gov/products/gao-25-107088>.

coordinated public awareness campaigns to help consumers recognize scams, reduce the stigma of victimization, and drive useful action such as reporting scams to a national law enforcement portal.

- **Assess potential benefits of establishing a U.S. National Anti-Scam Center.** Commission a study to determine the merits of creating a national hub that combines a reporting portal with professional training, public awareness, and victim support resources. A useful example of something similar is the National Center for Missing and Exploited Children (NCMEC), a private non-profit organization established by President Ronald Reagan.

For the full report and recommendations, see:

<https://fraudtaskforce.aspeninstitute.org/nationalstrategy>.
