JEC JOINT ECONOMIC COMMITTEE MINORITY

Combating the Global Scam Industry:

The Need for Stronger Government and Private-Sector Action

Image credit: Federal Bureau of Investigation (March 2026)

Ranking Member Maggie Hassan and Senior House Democrat Don Beyer

Joint Economic Committee Minority Report | October 27, 2026

Combating the Global Scam Industry: The Need for Stronger Government and Private-Sector Action

Executive Summary

In June 2025, Joint Economic Committee (JEC) Ranking Member Maggie Hassan launched a comprehensive initiative to combat scams that target Americans, which has included bipartisan investigations into the roles that private industries and federal agencies play in combating scams. In December 2025, JEC Chairman Schweikert, Vice Chairman Schmitt, Ranking Member Hassan, and Rep. Beyer sent requests regarding scam prevention efforts to the Federal Trade Commission (FTC), the Department of Homeland Security (DHS), the Department of Justice (DOJ), the Department of State, and the Department of the Treasury.[1] As part of this effort, JEC held a hearing entitled "The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters" on March 25, 2026.[2] For the first time in the second Trump Administration, federal officials – including representatives from the Federal Bureau of Investigation (FBI), FTC, and the multi-agency Scam Center Strike Force – testified about efforts to protect consumers and combat overseas scam compounds that target Americans.

These overseas scam compounds – which operate in Southeast Asia, are run by Chinese organized crime syndicates, and are staffed with trafficked persons held against their will – perpetrate fraud on an industrial scale.[3] According to reporting in the summer of 2026, more than two dozen new suspected scam compounds in Myanmar were rebuilt or expanded in the first half of this year, indicating "how a purported crackdown on the sites last year did little to stop the highly lucrative scamming industry."[4] The *Associated Press* also reported in September 2026 that although the Cambodian government has closed many large compounds, officials have taken comparatively fewer steps to dismantle the criminal organizations running scams.[5] The Treasury Department has reported that Americans lost at least $10 billion in 2024 to these operations.[6] Overall, both FTC and FBI have reported troubling scam trends in recent years, including growth in financial impact per victim, fraud reports and losses, and victimization and losses related to cryptocurrency investment scams, specifically.[7]

Based on written agency responses, testimony that officials provided at the March 2026 hearing, and staff interviews with experts, the Committee – Minority recognizes steps forward in federal efforts to combat overseas scam compounds. At the same time, the Committee – Minority has identified several ways in which federal agencies have fallen short of effectively fighting the evolving scams threat, as well as the ongoing need for better coordination between the private

and public sectors. This report includes recommendations that federal officials and other experts provided for addressing these shortcomings and strengthening measures to protect Americans from industrialized fraud.

Key Finding: Federal Agencies Have Taken New Steps to Combat Overseas Scam Compounds in Recent Years

- The Office of the U.S. Attorney for the District of Columbia, DOJ, FBI, the U.S. Secret Service (USSS), and other agencies launched the Scam Center Strike Force in November 2025. The Strike Force has worked to seize and disable U.S.-based infrastructure that supports scam compound operations; identify and bring charges against those who lead compounds; and trace and seize stolen cryptocurrency funds with the goal of returning them to Americans.
- At the Department of the Treasury, the Office of Foreign Assets Control (OFAC) has applied sanctions against hundreds of individuals and entities involved with the scam industry, and the Financial Crimes Enforcement Network (FinCEN) has partnered with U.S. and international partners to help victims and institutions recover funds stolen through cyber-enabled crimes.
- The Department of State maintains 60 employees in the United States and in the East Asia and Pacific region who dedicate significant time to efforts to combat overseas scam compounds. Concerningly, however, Committee – Minority staff received information from USSS indicating that a Department review of foreign assistance in 2025 eliminated at least one program that supported efforts in Bangladesh to combat scams. Despite the scope of the scams threat, State also indicated to the Committee – Minority that "the Department has the tools it needs to combat the threat internationally," and it did not describe any necessary legislative reforms to improve its response to scam compounds.[8]
- FTC has worked to disrupt the U.S.-based infrastructure that enables overseas scammers through aggressive civil enforcement, public-private partnerships, consumer reporting and data sharing, and coordination with domestic and international law enforcement. FTC also reported a significant recent increase in consumer relief from its fraud enforcement actions – around $1.83 billion in consumer redress in FY 2025 compared to $559 million in FY 2024.
- DHS has implemented a strategy centered on extensive public-private and international partnerships to identify and disrupt scam infrastructure, trace illicit financial flows, and support overseas enforcement. USSS, for example, sent more than 5,800 requests to Internet domain registrars to voluntarily take down domains involved in fraud between October 2024 and February 2026. (DHS did not, however, indicate how many registrars complied with these requests.) USSS also returned more than $770 million to victims of a variety of fraud schemes through assets seizures in FY 2025 and FY 2024.

Key Finding: Significant Weaknesses Remain in Federal Efforts to Coordinate Action, Support Victims, Collaborate with the Private Sector, and Measure Scam Impacts

- The United States still lacks a unified, government-wide strategy for combating scams. Instead, agencies, Congress, industry, and law enforcement largely operate in parallel rather than under a common strategic framework.
- A lack of centralized reporting for scams victims is a significant weakness. Victims face confusing reporting systems, stigma, and poor coordination among agencies.
- Although the federal government has established numerous partnerships with private-sector actors, these relationships remain fragmented, voluntary, and insufficiently integrated into a coordinated national effort.
- Federal communication and collaboration with state and local law enforcement needs to improve. Local agencies are often the first point of contact for victims but frequently lack the training, resources, and information-sharing mechanisms needed to flag transnational criminal activity for federal authorities tasked with combating overseas scam compounds.
- In some cases, federal officials lack the information necessary to identify the personnel and budget dedicated to addressing scam compound activity, specifically, or determine which scam attempts and losses arise from these operations. Improved data collection and reporting about scams would help federal agencies target prevention efforts and direct a unified government strategy.

Key Finding: Opportunities Exist for Congress and the Administration to Improve Federal Efforts

- Congress should pass the ReportScams.Gov Act to mandate a unified federal strategy to combat scams and establish a central location for Americans to find information and assistance regarding scams.
- Congress should consider legislation to improve the ability of law enforcement to hold scammers accountable, including by disrupting scam compound operations, pursuing justice against the heads of criminal organizations who direct scam activities, and working to support victims of scams.
- Congress and the Administration should identify ways to work together with private sector actors to proactively detect, address, and report abuses of their services, including through greater cooperation and information sharing with federal law enforcement partners.
- The Administration should strengthen and coordinate diplomatic pressure on Southeast Asian governments to uphold the rule of law and identify, disrupt, and dismantle scam compounds through law enforcement cooperation, information sharing, and joint

planning. Relatedly, Congress should pass the Scam Compound Accountability and Mobilization Act, which would require a federal strategy to hold accountable countries that enable or permit compound operations and enhance the capabilities of partner governments and law enforcement agencies to stop scam compounds.[9]

- Federal law enforcement should improve outreach, training, and information sharing efforts to ensure that state and local law enforcement are adequately supported as they confront scams in their jurisdictions and can identify, document, and refer scam compound activity to federal authorities.

Taken together, these recommendations provide a roadmap for future federal efforts to protect Americans from sophisticated and highly organized scams. No single action — or entity — will eliminate overseas scam compounds. But a more coordinated response that enables federal authorities to work with the private sector so that they can leverage businesses' information and technical capabilities could make it much harder and more costly for criminals overseas to victimize Americans.

Introduction and Background

Financial scams impose an enormous cost on the global economy and directly threaten the financial security of Americans. By one estimate, worldwide losses to scams in 2025 rivaled the cost of the global drug trade,[10] and estimates for annual losses for Americans in recent years range as high as $261.5 billion.[11] The financial impact per U.S. victim has also increased sharply, with dollar losses rising roughly 350% since 2019, according to the Federal Bureau of Investigation (FBI).[12] The Federal Trade Commission (FTC) has also reported substantial increases in fraud reports in 2025 compared to previous years and has found that fraud losses for consumers have grown nearly 430% since 2020.[13]

As the AP/Frontline documentary *Scammed* reported in September 2026, the rise of overseas scam compounds operating in Southeast Asia has played a critical role in driving these disturbing trends.[14] In Myanmar, Cambodia, and Laos, these compounds – run by Chinese organized crime syndicates and staffed with trafficked persons held against their will – perpetrate fraud on an industrial scale.[15] Among other schemes, this fraud includes "pig butchering" scams, which cultivate victims over time and convince them to deposit substantial funds into fraudulent investments.[16] Notably, the U.S.-China Economic and Security Review Commission has explained that these operations have spread in the region with at least the implicit backing of actors in the Chinese government, which has used the scam crisis to increase its regional influence.[17] Selective enforcement by the Chinese government – focused only on compounds that target Chinese citizens – has also driven scammers' shift toward U.S. victims.[18]

This activity has had a devastating impact on Americans. According to FBI, victimization and losses from investment fraud increased 1,725% and 3,793%, respectively, from 2019 to 2025, "driven by the scalable industrialized scam compound model and the widespread use of cryptocurrency."[19] In total, the Treasury Department has reported that Americans lost at least $10 billion in 2024 to scam operations based in Southeast Asia.[20] Host countries for these operations, in turn, have received as much as 40 percent of their gross domestic product (GDP) from scam revenue, and the Chinese crime syndicates themselves have earned more than $40 billion annually.[21]

Scam compounds craft convincing schemes and reach Americans using U.S.-based infrastructure and platforms, including social media to target victims; satellite providers and VPN networks to connect to the internet; and hosted domains to support websites that appear more legitimate for U.S. users.[22] Scammers also use American-owned AI platforms to scale their operations, create convincing fake profiles, develop tailored content, and operate in different languages.[23] To connect with victims, scam compounds also rely on spoofed phone calls and SMS phishing campaigns through U.S. telecommunications carriers.[24] The Department of Justice (DOJ) has explained to the Committee that "[t]hese abuses of U.S. infrastructure and platforms degrade their reliability for the American people."[25]

The exploitation of U.S. technology also underscores the importance of a comprehensive, whole-of-society approach with strong coordination among federal agencies and collaboration between the public and private sectors. The Scam Center Strike Force, created in November 2025 and led by DOJ, has worked with multiple federal agencies to prosecute scam compound leaders, support sanction actions, seize illicit funds, and disable the U.S.-based infrastructure that supports scam compounds.[26] Relatedly, in March 2026, President Trump issued an executive order entitled "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens," which directed federal agencies to create an action plan to disrupt criminal organizations operating scam compounds.[27] The order also directed the creation of an operational cell within the National Coordination Center to coordinate these efforts, including through collaboration with the private sector as appropriate.[28]

To assess federal efforts to combat scam compound activity, Chairman Schweikert, Vice Chairman Schmitt, Ranking Member Hassan, and Rep. Beyer sent requests to FTC, the Department of Homeland Security (DHS), DOJ, the Department of State, and the Department of the Treasury in December 2025.[29] These requests sought information on collaboration with U.S. companies and other agencies, budget and staff devoted to addressing scam compounds, and additional tools to enhance effectiveness, among other issues.[30] The Joint Economic Committee also held a hearing entitled "The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters" on March 25, 2026.[31] For the first time in the second Trump Administration, federal officials – including representatives from FBI, FTC, and the

Scam Center Strike Force – testified about efforts to combat scam compounds and protect Americans.

Drawing in part on this hearing testimony, Ranking Member Hassan and Senator Rick Scott introduced the ReportScams.Gov Act in June 2026.[32] This legislation would mandate a unified federal strategy to combat scams and establish a central location for Americans to find information and assistance regarding scams.[33]

The report below presents insights and recommendations from the March 2026 hearing and the Committee – Minority's investigation, which highlight certain federal efforts but also the need for greater collaboration, support for victims, and engagement with the private sector. The persistent nature of the economic threat from scam compounds underscores the urgency of these efforts. According to reporting in July 2026, for example, more than two dozen new suspected scam compounds in Myanmar were rebuilt or expanded in the first half of this year, indicating "how a purported crackdown on the sites last year did little to stop the highly lucrative scamming industry."[34] In response to this ongoing challenge, federal approaches must grow and evolve, and Congress must continue to pursue new measures to protect Americans.

Federal Agencies Have Taken New Steps to Combat Scams

In written responses to Committee requests, FTC, DHS, DOJ, the Department of the Treasury, and the Department of State described actions to combat overseas scam compounds, including through coordination between agencies and engagement with the private sector. Several agencies also recommended changes to enhance federal efforts, including stronger diplomatic pressure on Southeast Asian governments; improved oversight and accountability for U.S. telecommunications and social media companies; modernized approaches for recovering stolen digital assets; and simplified methods for prosecuting scam compound operators and seizing their assets. In addition, certain agency responses indicated that federal officials lack the information necessary to determine which scam attempts and losses correspond to scam compound activity, specifically, or the personnel and budget dedicated to this issue.

Federal Trade Commission

In its response to the Committee, FTC emphasized efforts to disrupt the U.S.-based infrastructure that enables overseas scammers through aggressive civil enforcement, public-private partnerships, consumer reporting and data sharing, and coordination with domestic and international law enforcement.[35] In FY 2025, FTC brought 40 law enforcement actions involving fraudulent schemes, including unlawful robocalls, investment scams, and technical support scams.[36] Overall, FTC reported obtaining significant consumer relief from fraud enforcement actions, securing around $559 million in consumer redress in FY 2024 and $1.83 billion in FY 2025.[37]

As part of this work, FTC has prioritized enforcement actions against companies in the United States that facilitate foreign schemes. For example, FTC brought a case in 2025 against Paddle, a U.K. payment processor operating in the United States that collected payments on behalf of tech-support scammers overseas.[38] In addition, FTC has worked with the Industry Traceback Group and other partners to "traceback" illegal calls and identify the providers responsible for allowing scammers to access U.S. communication networks.[39] As part of this project, FTC sent 30 warning letters to service providers responsible for this communications traffic, "significantly disrupting…overseas scams which included government and business imposters."[40] In 2023, for example, FTC noted that almost all the providers targeted in its outreach had significantly curbed or fully stopped the flow of illegal robocalls into the United States over their networks.[41] Through challenges under the America Competes Act, FTC has also encouraged the private sector to develop technological solutions to combat robocalls, other telemarketing fraud, and AI-enabled voice cloning schemes.[42]

FTC also described cooperation with DOJ on cross-border fraud cases – in one example, FTC assisted with a DOJ criminal matter involving two Jamaican citizens running a lottery scam – and the two agencies have run parallel criminal and civil law enforcement actions.[43] FTC also refers consumer reports that involve high dollar losses to the FBI's Internet Crime Complaint Center Recovery Asset Team when the consumer agrees to the referral and it meets FBI criteria.[44] Through this process, FBI can notify bank partners in an attempt to freeze funds sent to scammers.[45] FTC reported that it referred almost 700 reports to this FBI team in 2024.[46] (FTC did not provide a breakdown of the resolution of these cases, but a 2025 FTC report noted several success stories in which this process froze wire transfers that older adults had initiated during scams.[47]) Finally, FTC operates the Consumer Sentinel Network, which collects consumer reports about fraud, scams, and business practices and shares data with law enforcement professionals, including DOJ and other agencies addressing overseas scam compounds.[48] Reporting parties to the Consumer Sentinel Network include individuals, law enforcement agencies, financial institutions, and communications platforms.[49]

FTC also described limitations in its ability to conduct international law enforcement actions and track factors related to overseas scam compounds specifically. FTC noted, for example, that gathering evidence abroad can involve burdensome procedures that vary by country, and many jurisdictions will refuse to enforce judgments that involve civil penalties.[50] In addition, because FTC primarily focuses on disrupting U.S.-based facilitators of foreign scams, the agency noted that its actions affect "a wide swath of foreign scams without distinguishing based on country or region of origin."[51] As a result, "FTC cannot specifically identify which of its fraud matters are connected to a scam compound."[52] FTC answers in response to Committee questions therefore focused on efforts to disrupt foreign actors more broadly and not efforts that address scam compounds in particular.[53] FTC also could not provide estimates of the total budget or staff dedicated to combating scam compound activity or the funds it has recovered that are specifically associated with these operations.[54]

Finally, FTC Chairman Andrew N. Ferguson provided several recommendations for Congressional actions that could assist agency efforts to recover funds for consumers, address scams on telecommunications and social media platforms, and collaborate with foreign partners, including:

- Authorize courts to award monetary relief in FTC enforcement actions under Section 13(b) of the FTC Act, which allows FTC to go directly to a federal court when it believes a party is violating or about to violate the law.[55] The U.S. Supreme Court held in 2021 that Section 13(b) does not authorize courts to grant monetary relief in FTC enforcement actions, and FTC noted for the Committee that "the loss of this authority has made it much more difficult for the FTC to obtain monetary redress for consumers."[56]
- Make permanent the U.S. SAFE WEB Act, which is set to expire in September 2027.[57] Passed by Congress in 2006, the U.S. SAFE WEB Act affirms FTC authority to pursue deceptive or unfair practices involving foreign actors targeting Americans.[58] The law has also provided FTC with enhanced tools for cross-border enforcement, including in the areas of information sharing and investigative assistance.[59] FTC has argued that "a lapse of such legislation would deprive the FTC of its clear authority to pursue fraudulent and other harmful conduct relating to foreign commerce, likely having a dramatic impact on U.S. consumers."[60]

Department of Homeland Security

DHS reported that it has implemented a strategy centered on extensive public-private and international partnerships to identify and disrupt scam infrastructure, trace illicit financial flows, and support overseas enforcement.[61] DHS also highlighted asset recoveries for scam victims and called for expanded authorities and stronger collaboration to combat increasingly sophisticated scam networks.[62] First, DHS described regular engagement with a variety of private sector actors that "are victims of fraud or provide services that may be abused in illicit schemes."[63] The U.S. Secret Service (USSS), for example, sent more than 5,800 requests to Internet domain registrars to voluntarily take down domains involved in fraud between October 2024 and February 2026.[64] (DHS did not however, indicate how many registrars complied with these requests.) DHS also noted that blockchain analytics companies have provided useful data and tools to enable the Department to detect and address illicit activity.[65]

In terms of collaboration across the federal government, DHS reported that USSS and Homeland Security Investigations (HSI) have collaborated with partners as part of the Scam Center Strike Force, described in more detail below.[66] USSS has also partnered with FBI to notify victims of cryptocurrency scams and mitigate their losses.[67] In addition, USSS has collaborated with cryptocurrency investment firms to recover millions of dollars in digital assets used in transnational fraud operations.[68] DHS stated that USSS had returned more than $770 million to fraud victims through assets seizures in FY 2025 and FY 2024, although these efforts related to "a range of fraud schemes" and were "not limited to foreign scam compounds specifically."[69] HSI

has also investigated financial fraud networks linked to overseas scam compounds in Southeast Asia and related technology and helped return assets to victims of fraud, including romance, investment, and business email compromise scams, through the DOJ Asset Forfeiture Program.[70] Across all activities in FY 2024, HSI also reportedly seized more than $886 million in criminally derived currency and assets and $192 million in virtual currency.[71]

Regarding international cooperation, DHS explained that it has worked with a variety of foreign governments and law enforcement, including the Royal Thai Police, and collaborated with the State Department to deliver 20 cyber-related courses to 607 participants from these partners in FY 2024 and FY 2025.[72] DHS also described efforts at the HSI Cross-Border Financial Crime Center to establish a Counter Threat Finance Unit, designed to enhance HSI capacity to disrupt financial activities associated with national security threats.[73] (A July 2026 statement from HSI regarding a nationwide operation against illegal SIM box operations noted that the Counter Threat Finance Unit would analyze seized data to identify victims, quantify losses, and trace illicit proceeds.[74]) In addition, DHS also stated that it is collaborating with the State Department to initiate a "Contact Group" composed of U.S. allies and partners "to fight Asia-based Criminal Scam Groups."[75]

Finally, DHS offered several recommendations to improve federal and private sector efforts to combat criminal scam networks, including:

- Incentivize providers of information and communications services to Americans to proactively detect and address abuse of the services that they provide while also protecting user privacy. This incentive could mirror existing requirements for financial institutions to report suspicious activity under the Bank Secrecy Act.[76]
- Improve oversight by private sector telecommunications companies regarding the sale of large quantities of SIM cards to individuals or groups.[77] HSI has explained that "SIM farms" house hundreds or thousands of cellphone SIM cards, facilitating activities like scam calls, phishing texts, and other fraud schemes that cost Americans around $15 million per year.[78] DHS stated that telecommunications companies can also improve their ability to identify smishing attacks – deceptive text messages sent to smart devices – and trace these attacks to their origin.[79]
- Update laws to improve the ability of U.S. law enforcement to recover digital assets and investigate illicit financial activity. DHS also referenced the need for expanded authorities to investigate new forms of criminal activity involving digital assets.[80]
- Strengthen and coordinate diplomatic pressure on Southeast Asian governments to identify, disrupt, and dismantle scam compounds through law enforcement cooperation, information sharing, and joint planning. According to DHS, changes in foreign assistance could serve as leverage to incentivize meaningful action by host countries to close compounds and cooperate with U.S. and international partners. DHS also noted that

"access to targeted traveler records in Southeast Asia with assistance from host governments" would greatly benefit ongoing investigations, given frequent travel in the region by members of criminal syndicates.[81]

Department of Justice

In testimony before the Committee, representatives from DOJ emphasized the critical role of the Scam Center Strike Force, a collaboration between the Office of the U.S. Attorney for the District of Columbia, DOJ Criminal Division, FBI, USSS, and other agencies created in 2025.[82] Among other goals, the Strike Force seeks to seize and disable U.S.-based infrastructure that supports scam compound operations; identify and charge leaders of compounds; and trace and seize stolen cryptocurrency funds with the goal of returning them to Americans.[83] The Strike Force includes embedded Department of Defense staff, and it also routinely partners with the Department of State, the Office of Foreign Assets Control at the Treasury Department, and the Department of Commerce.[84] DOJ representatives also reported that the Strike Force has actively worked with foreign law enforcement partners, including the Royal Thai Police.[85] DOJ has also partnered with the Department of State to operate the U.S. Transnational and High-Tech Crime Global Law Enforcement Network, which assists international partners with investigating and prosecuting transnational organized crime.[86]

Through its efforts, the Strike Force has seized websites, Starlink terminals, and a Telegram channel used by scam compounds; prosecuted scam compound leaders; and frozen or seized hundreds of millions in cryptocurrency assets.[87] As of September 2026, the Strike Force reported that it had restrained — effectively frozen — more than $930 million in cryptocurrency from schemes that originated in scam compounds.[88] DOJ has also pursued separate actions against scam compound proceeds, including a forfeiture action against $15 billion in cryptocurrency proceeds of the Prince Holding Group in October 2025.[89]

The Strike Force has also partnered with private industry, including social media platforms, satellite internet providers, and internet services providers to block access for scam centers and prevent the exploitation of U.S.-based infrastructure.[90] In May 2026, for example, the Strike Force conducted a "disruption week" in which "the private sector took voluntary action to interrupt millions of social media, email, and internet access accounts used by transnational organized crime actors in Southeast Asia to defraud Americans."[91] Among other activities, participants interrupted malicious IP address traffic and network connections, decommissioned servers and hosting infrastructure, and disrupted activity across social media and email accounts.[92] During this week, federal authorities also shared information that allowed private sector representatives to freeze more than $3.8 million in cryptocurrency connected to funds stolen from Americans.[93]

FBI also highlighted additional initiatives to collect information on scams and mitigate losses for victims. The FBI's Internet Crime Complaint Center (IC3), for example, aggregates complaints

from scam victims, issues public advisories and annual reports, and distributes investigative referrals to domestic and international partners.[94] In terms of minimizing victim harm, through the "Operation Level Up" initiative, the FBI calls victims who are actively being defrauded and informs them of the scam activity.[95] According to FBI, 77 percent of these individuals were unaware that they were being scammed, and the operation has saved victims more than $529 million as of March 2026.[96] The operation also identified more than 1,600 scam domains, emails, numbers, and accounts for a variety of companies and froze or seized more than $101 million in cryptocurrency.[97] The IC3 Recovery Asset Team has also worked with financial institutions to freeze fraudulent wire transfers, and in 2025, the team handled around 3,900 incidents, representing more than $1.1 billion in attempted theft, and froze more than $679 million.[98] FBI also reported, in general, that it returned more than $336 million to scam victims in 2025.[99]

Finally, DOJ representatives identified several recommendations for Congressional action to help law enforcement officials prosecute the leaders of organized criminal scam enterprises, including scam compounds; quickly take down scam websites that defraud Americans; and more efficiently provide compensation to scam victims.[100] Regarding compensation, Karen Seifert, Director of the Scam Center Strike Force, explained that current federal law related to the treatment of cryptocurrency seizures made the process for remitting these funds to victims slow, resource-intensive, and unlikely to make most victims whole.[101] The AP/Frontline documentary *Scammed* similarly noted in September 2026 that, in general, scam proceeds held by the federal government are not flowing back to victims.[102] Ms. Seifert stated, however, that DOJ is using all the tools at its disposal to assist victims, including through seeking Congressional action to reduce victimization from cyber scams.[103]

Department of State

In response to Ranking Member Hassan, the State Department described combating online scam operations that target American citizens as a top priority and outlined a five-part strategy that combines foreign assistance, sanctions and other regulatory measures, diplomacy, interagency coordination, and partnerships with the private sector to disrupt transnational criminal organizations.[104] State has roughly 60 employees in the United States and in the East Asia and Pacific region who "dedicate a significant portion of their time to efforts to combat overseas scam compounds."[105] In terms of intergovernmental cooperation, State reported close collaboration with the Scam Center Strike Force and daily contact with DOJ, DHS, and the Department of the Treasury.[106]

Regarding foreign assistance efforts, State explained that its Bureau of International Narcotics and Law Enforcement Affairs (INL) enables DOJ and DHS to train foreign counterparts to address scam threats and conduct joint operations.[107] State reported that it had around "$74 million in International Narcotics Control and Law Enforcement (INCLE) and Economic Support Fund (ESF) resources allocated to combat overseas scam compounds and plans to allot additional funding to combat online scam operations."[108] As of May 2026, State reported "numerous

seizures and disruptions totaling in the low hundreds of millions of dollars" connected to efforts from foreign law enforcement agencies receiving Department-funded support.[109] For specific dollar amounts and attributions, however, State "respectfully [referred the Committee] to the Departments of Justice, Homeland Security, and Treasury."[110]

Concerningly, Committee – Minority staff received information from USSS indicating that a State Department review of foreign assistance in 2025 eliminated the USSS Counterterrorism Finance Mentorship Program in Bangladesh.[111] According to USSS, this program was developed to provide training to core financial investigators in the country, which increased investigative capacity to target cyber-enabled fraud, among other crimes.[112] Specifically, in a program operating between 2023 and 2025, USSS and State conducted cryptocurrency training for the Bangladesh Criminal Investigative Division.[113] In 2025, however, before the completion of training, USSS was notified that the program was being cancelled, even with the full support of the U.S. ambassador to Bangladesh, due to an overall program review by State.[114] USSS noted to Committee – Minority staff that this elimination occurred at a critical time during a changeover in the Bangladeshi government.[115] Despite these setbacks, in March 2026, Bangladeshi authorities successfully recovered around $3.6 million in cryptocurrency funds stolen in connection with a scam that lured investors through false promises of high returns.[116] In a letter to the U.S. ambassador dated April 2, 2026, the chief of the Bangladesh Criminal Investigative Division stated that the recovery "reflects the strong cooperation between Bangladesh and the United States in addressing cyber enabled transnational crime."[117] The elimination of this program despite its evident value, however, raises the concern that State did not fully consider the impact of its program cuts on international scam prevention efforts.

Regarding its engagement with the private sector, State reported that it "primarily engages with Google, Meta, TRM Labs, and Starlink, as well as various entities like Visa, MasterCard, TikTok, and online dating platforms like the Match Group."[118] These efforts include activities to build relationships between companies and law enforcement to share information and mitigate the risk of misuse of these platforms by scammers to defraud consumers and recruit trafficking victims.[119]

On the international level, the U.S. Mission to the Association of Southeast Asian Nations (ASEAN) has worked to operationalize the U.S.-ASEAN 10 Public-Private Partnership Principles for Tackling Online Scams, which discuss enhancing information sharing across sectors and borders.[120] State has also coordinated on these issues at the ASEAN Senior Officials' Meeting on Transnational Crime and the ASEAN Regional Forum and has worked with INTERPOL and U.N. agencies like the U.N. Office on Drugs and Crime and the International Office for Migration.[121]

Finally, despite the scope of the scams threat, State indicated that "the Department has the tools it needs to combat the threat internationally" and did not describe any necessary legislative reforms to improve its response to scam compounds.[122] State, however, did note that "additional

support from Congress to further raise public awareness of this serious threat would be especially valuable."[123]

Department of Treasury

In its response to the Committee, the Department of the Treasury described a coordinated strategy to disrupt transnational scam operations through anti-money laundering tools, international financial engagement, and aggressive sanctions against individuals and entities involved with scam compound activity. First, Treasury explained that the Financial Crimes Enforcement Network (FinCEN) alerts financial institutions and law enforcement regarding ongoing scams and partners with U.S. and international partners to help victims and institutions recover funds stolen through cyber-enabled crimes.[124] These efforts include analyses of Bank Secrecy Act (BSA) data to determine trends, devise leads for law enforcement, and support law enforcement investigations.[125] Most recently, in September 2026, FinCEN issued an analysis and an alert urging financial institutions to remain vigilant regarding digital asset investment scams perpetrated by overseas scam compounds.[126] FinCEN identified nearly $13 billion linked to suspected digital asset scams based on BSA reports filed between September 2023 and December 2025.[127]

FinCEN also works to block international entities engaged in money laundering from accessing the U.S. financial system.[128] In 2025 and 2026, for example, FinCEN severed access for the Cambodia-based Huione Group and its successor entities, which have laundered proceeds from North Korean cyber heists and transnational criminal organizations operating scams in Southeast Asia.[129] Finally, FinCEN has also helped U.S. victims of cyber-enabled fraud and their financial institutions recover lost funds through the Rapid Response Program (RRP), a joint effort by FinCEN, U.S. law enforcement partners, and foreign partners.[130] Through RRP, FinCEN can quickly share financial intelligence with counterpart intelligence units and encourage foreign authorities to halt and repatriate fraudulent transactions.[131] Treasury reports that since its creation in 2015, RRP has facilitated the interdiction of more than $1.8 billion and the recovery of more than $1 billion in stolen proceeds on behalf of 5,790 U.S. victims.[132]

Through the Office of Terrorist Financing and Financial Crimes, Treasury also conducts outreach to international partners to identify opportunities to disrupt the financial networks of scam compounds.[133] In addition, this office publishes the National Money Laundering Risk Assessment, which highlights threats from fraud networks.[134] Finally, in response to questioning from Ranking Member Hassan in July 2026, Under Secretary of the Treasury for International Affairs Erin Browne noted that the United States would discuss combating financial fraud during its current presidency of the G20 and future presidency of the G7.[135] In a statement in September 2026, for example, G20 finance ministers and central bankers welcomed efforts to address "the evolving threat emanating from scam compounds and exploitation of AI by fraudsters," including actions to strengthen public-private partnerships and information sharing.[136]

Importantly, the Office of Foreign Assets Control (OFAC) has applied sanctions against individuals and entities involved with the scam industry and routinely partners with law enforcement agencies, through the Scam Center Strike Force, to identify additional targets.[137] According to Treasury, OFAC has taken action against more than 200 entities and individuals involved in overseas scam compounds since January 2025.[138] In April 2026, for example, OFAC designated Kok An – a Cambodian senator who controlled scam compounds – and 28 other individuals and entities in his network, which reportedly stole millions from U.S. victims.[139] Treasury undertook these actions in coordination with the Scam Center Strike Force.[140] In June 2026, OFAC also sanctioned nine individuals and 26 entities linked to the Prince Group Transnational Criminal Organization, which has generated "substantial profits from scam compounds where fraud operations target victims in the United States and around the world."[141] Finally, in September 2026, OFAC sanctioned the transnational criminal organization Xinbi Guarantee, which operates a large online marketplace, based in Southeast Asia, that connects scam compound operators with services to support their criminal enterprises.[142] Treasury has noted that Xinbi Guarantee has processed the equivalent of more than $24 billion in digital assets and fiat currency through its platforms since its inception in 2022.[143]

The JEC Hearing Spotlighted Serious Shortcomings in Federal Scam Prevention Efforts

During the Committee hearing in March 2026, federal law enforcement officials testified for the first time in the second Trump Administration about efforts to combat overseas scam compounds. Experts from the Aspen Institute, AARP, and the Government Accountability Office (GAO) also testified.

In these remarks, several common themes emerged about areas for improvement in the current federal strategy. First and most importantly, witnesses explained that the United States still lacks a unified, government-wide strategy for combating scams. Several witnesses also raised that victims face confusing reporting systems, stigma, and poor coordination among agencies. In addition, experts and officials noted that federal coordination with the private sector remains fragmented and voluntary, and federal communication and coordination with state and local partners should improve as well. Witnesses also explained that the lack of a standard scam definition, the absence of a government-wide estimate of scam losses, and various barriers to information sharing have undermined federal efforts. Finally, experts and officials described a need to modernize federal legal authorities and private sector prevention methods to keep pace with evolving scam threats.

In March 2026, President Trump issued an executive order entitled "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens," which directed federal agencies to create an action plan to disrupt criminal organizations operating scam compounds.[144] The order

also directed the creation of an operational cell within the National Coordination Center to coordinate these efforts, including through collaboration with the private sector as appropriate.[145] Although this push for greater federal planning and coordination is a step forward in the fight against scam compounds, Congress should continue to strengthen federal coordination, information sharing, and support for victims. As Kate Griffin of the Aspen Institute explained to the Committee, "[i]t 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."[146] The findings below provide a roadmap for this kind of Congressional action to protect Americans.

The United States lacks a coherent whole-of-government strategy to combat scams. Witnesses explained that the United States still lacks a unified, government-wide strategy for combating scams. Instead, agencies, Congress, industry, and law enforcement largely operate in parallel rather than under a common strategic framework. Seto Bagdoyan of GAO, for example, explained that officials from 13 federal agencies "were not aware of a government-wide, or national, strategy to guide government efforts to combat scams."[147] In addition, research by GAO into this topic "did not identify an existing strategy that could be used government-wide to counter scams."[148] Instead, Mr. Bagdoyan noted, "each agency has its own mandate and authority, with each largely carrying out activities related to countering scams independently."[149] In general, Mr. Bagdoyan explained that the scams threat to U.S. consumers "requires an equally immediate, decisive, and comprehensive federal response. […] The solution starts with a strategy. There is no way around this."[150]

Ms. Griffin of the Aspen Institute also called for a national strategy to combat scams with dedicated resources and broad coordination mechanisms.[151] While Ms. Griffin acknowledged that certain measures to combat scams will occur naturally in the private sector, she explained that "[m]uch of it will not happen unless Congress and the Executive Branch take coordinated action to empower it."[152] Similarly, Kathy Stokes, Senior Director of Fraud Prevention Programs at AARP, stated that "we really need a national fraud strategy…that coordinates everything."[153] Although FTC Associate Director Lois Greisman did not address this issue in her testimony, Mr. Bagdoyan noted that FTC officials have expressed to GAO that "a government-wide strategy could help overcome…jurisdictional barriers, if significant resources could be applied to tackle multifaceted and evolving scams" [154]

Regarding ongoing federal efforts to establish a unified strategy to combat scams, Mr. Bagdoyan explained that FBI had outlined actions to address this recommendation from GAO.[155] In October 2025, for example, FBI stated that these actions would include establishing a multi-agency working group to create an international center of excellence to address cyber-enabled fraud; interagency cooperation to explore relevant regulatory reforms; and partnerships with the private sector on fraud detection and prevention.[156] Mr. Bagdoyan noted, however, that it was

not clear whether the working group would "lead to any restructurings either at the FBI or any of the other lead agencies."[157] He also explained that "[w]hile the CFPB, FTC, and FBI described actions they plan to take to implement our recommendations, they did not specify whether any of these are under way or when they might be initiated."[158]

A lack of centralized reporting for victims remains a significant problem. Several witnesses argued that victims face confusing reporting systems, stigma, and poor coordination among agencies. GAO has previously noted that eight federal agencies receive complaints from consumers about scams, and Mr. Bagdoyan explained that improving scam complaint reporting could help agencies target their efforts and measure progress.[159] Ms. Stokes also stressed that "it is important to streamline victim reporting, which is currently received by agencies on an agency-by-agency basis, leaving victims confused about who to report to."[160] Ms. Stokes also recommended measures to improve responsiveness to victims, noting that when individuals report to FBI IC3, "they don't know if anyone received it or not because there is no kind of a closure loop there."[161] She stated that a "front door" for reporting would "go a really long way," emphasizing that "we would also have to know that those reports are going to law enforcement, and that [victims] are hearing back that something is being done."[162] Relatedly, Ms. Griffin noted that Aspen Institute had recommended the "creation of a 'national front door' for scam reporting."[163]

This kind of streamlining is critical, Ms. Stokes explained, "because fragmented and confusing reporting systems prevent authorities from seeing the full scope and patterns of fraud."[164] She also noted that a "clear, accessible reporting process... ultimately increases the likelihood that cases are investigated, perpetrators are held accountable, and future victims are prevented."[165] In response to questioning from Ranking Member Hassan, both FBI Deputy Assistant Director Gregory Heeb and Ms. Greisman committed to simplifying the scam reporting process for Americans.[166]

Federal coordination with the private sector is fragmented, voluntary, and insufficiently integrated into a coherent national strategy. The federal government has established numerous partnerships with financial institutions, telecommunications providers, technology companies, social media platforms, cryptocurrency firms, and other private-sector actors. Witnesses, however, indicated that these relationships remain fragmented, voluntary, and insufficiently integrated into a coherent national strategy. Ms. Griffin, for example, stated that although "[c]ompanies are acting…[t]hey cannot succeed alone, and their capabilities will remain severely constrained and disjointed unless policymakers help them."[167] Commissioner Reva Price of the U.S.-China Economic and Security Review Commission also noted the need for "greater cooperation between the U.S. government and financial intermediaries to detect and stop scams, particularly relating to cryptocurrency."[168]

Karen Seifert, Director of the Scam Center Strike Force, further noted that cooperation with the Strike Force varies by company, and "it's up to [each company] to determine how much effort and energy to put behind these types of initiatives."[169] She also explained that, in the case of the

financial sector, "[w]e have a lot of banks that say, 'We want to help, but we don't really understand how to help,'" and banks may receive a victim report "that never comes over to the feds."[170] In general, Ms. Seifert described a range of engagement from the private sector, with certain parties open to cooperating with the Strike Force, "other ones that are maybe not as vocal about their openness of their cooperation, and then we have others that we are still working on."[171] Similarly, in response to questioning regarding private industry cooperation, Ms. Greisman stated that "[i]t can be uneven, it can be challenging."[172]

To address these kinds of gaps, Ms. Griffin recommended that Congress facilitate the sharing of actionable scam intelligence between government agencies and harmonize expectations across different industries.[173] She further explained that although companies are eager to report useful scam intelligence, "most of the ways that they have to report are too reliant on manual or even paper-based processes," highlighting the need for "a single portal for companies to report in bulk."[174]

Federal communication and collaboration with state and local law enforcement should improve. Witnesses repeatedly emphasized that local agencies are often the first point of contact for victims but frequently lack the training, resources, and information-sharing mechanisms needed to flag transnational criminal activity for federal authorities tasked with combating overseas scam compounds. Mr. Heeb, for example, stated that state and local law enforcement officials are "in a very challenging situation, and nobody would expect that most departments would be able to conduct an investigation of this scale."[175] Similarly, Commissioner Price noted that in many cases, these authorities "lack the training and resources to identify these cases as part of transnational criminal operations linked to China."[176] She also noted that "[t]oo often, cases are filed as isolated fraud incidents and never reach the federal investigators who could connect them to broader scam center networks."[177]

In this context, Ranking Member Hassan noted that New Hampshire law enforcement officials contacted by JEC staff were not even aware that the Strike Force existed.[178] (As of September 2026, these same law enforcement officials had not received outreach from the Strike Force.[179]) Ms. Seifert, in fact, acknowledged that "we haven't had that pathway [to state and local law enforcement] so far" because the Strike Force has focused on targeting overseas defendants.[180] She did, however, note that the Strike Force had exposure to state and local officials through FBI initiatives with embedded task force officers.[181] While describing FBI efforts to integrate and train state and local partners, Mr. Heeb suggested "using the task force model to sort of train the trainer, to get out and have our folks be the point of contact to train our state and local partners. Like I say, we have started that already, but we certainly need to do more in that area."[182]

Additional efforts in this area would be consistent with recommendations that Commissioner Price and Ms. Griffin provided. Commissioner Price, for example, recommended that Congress direct the Strike Force to "establish information-sharing mechanisms and training programs…that enable state and local agencies to identify, document, and refer scam center-linked cases to

federal authorities."[183] Similarly, Ms. Griffin noted the need for "more standardized training programs for state and local officials and, potentially, forming targeted federal-state collaborations or task forces to promote best practices and effective communication with the public."[184]

The federal government lacks a standard scam definition and government-wide estimate of scam losses, which undermines agency efforts. In his testimony, Mr. Bagdoyan explained that "there is no single, government-wide estimate of the total number of scams and financial losses. Similarly, federal agencies have not produced a common, government-wide definition of scams."[185] He attributed this result to a "lack of interest."[186] Mr. Bagdoyan also explained that "CFPB, the FBI, and FTC each can calculate an estimate of complaints they receive related to scams but not the exact number of scam complaints."[187] He further stated that improving "data collection and reporting about the types and extent of scams would help government agencies, Congress, and industry target their preventative efforts and measure progress in scam prevention and would inform an effective antiscam strategy."[188] For these reasons, GAO has specifically recommended that agencies harmonize their data collection and develop a single estimate of the number of consumers affected by scams, as well as dollar losses resulting from these activities, factoring in an estimate of unreported incidents.[189]

Notably, as mentioned above, several federal agencies could not provide the Committee with an estimate of amounts that they have recovered for consumers that are specifically attributable to losses from scam compounds. For example, although FTC stated that it obtained $1.83 billion in consumer redress in FY 2025, it could not "specifically identify which of its fraud matters are connected to a scam compound."[190] Similarly, DHS stated that through USSS, it had recovered financial losses of more than $1 billion in FY 2024 and FY 2025, including more than $770 million returned to fraud victims through asset seizures – but this total was "not limited to" efforts to combat foreign scam compounds specifically.[191] Finally, the State Department stated that "numerous seizures and disruptions totaling in the low hundreds of millions of dollars are connected to efforts from foreign law enforcement who received" support for training and sanction actions.[192] As mentioned above, however, for specific dollar amounts and attributions, the State Department "respectfully [referred the Committee] to the Departments of Justice, Homeland Security, and Treasury."[193]

Federal legal authorities and procedures have not kept pace with evolving scam threats. Several witnesses argued that certain legal and procedural barriers have made it more difficult to dismantle scam infrastructure, seize criminal assets, recover victim funds, and prosecute overseas operators. As noted above, DOJ witnesses pointed to limitations related to the seizure of digital assets that make it difficult to restore funds to victims; obstacles to holding scam compound leaders responsible for human trafficking; and barriers to seizing websites used in scam operations.[194] Ms. Griffin also cited a variety of recommendations in the Aspen Institute's

national scam prevention strategy that could enhance the powers of law enforcement to seize or achieve forfeiture of the digital assets of criminals and restore funds to victims.[195]

Underscoring the importance of this issue, Ms. Stokes testified that "victims face complex, slow, or opaque processes to recover even a portion of what was stolen, and in many cases receive nothing at all."[196] For this reason, AARP recommended that Congress strengthen mechanisms that prioritize returning funds to victims, remove tax penalties that effectively punish individuals who have been defrauded, and ensure that agencies have clear authorities to assist victims in recovery.[197] Commissioner Price also urged Congress to consider establishing a reward program that would incentivize "cryptocurrency tracing firms and other private sector actors to identify and report stolen assets linked to scam center operations."[198] She further suggested that when law enforcement successfully recovers scam center assets, "Congress should consider directing that the proceeds be prioritized for victim restitution rather than flowing into the general Assets Forfeiture Fund."[199]

Private sector actors should improve their preventive measures. Witnesses repeatedly argued that private-sector companies occupy key intervention points in the scam lifecycle and should focus more on preventing scammers from reaching victims, interrupting fraudulent payments, and deploying stronger technological safeguards. Richard Goldberg, Associate Counsel in the DOJ Criminal Division, for example, argued that communications platforms should improve their ability to prevent scammers from reaching victims through phone calls, texts, emails, and social media.[200] Ms. Seifert also stated that in addition to telecommunications companies providing scam warnings in connection with certain calls, "the next step is to not even allow that phone call to come through."[201] Mr. Goldberg also stated that banks, cryptocurrency firms, and other payment providers should be prepared to identify suspicious transactions and prevent fraudulent payments before funds leave victims' accounts.[202] (Ms. Seifert specifically noted that "there is no protection for [cryptocurrency exchanges] to do a freeze."[203]) Ms. Griffin also urged the private sector to improve identity verification, take down fraudulent websites, deactivate accounts of bad actors, share more actionable intelligence with law enforcement, and improve just-in-time warnings and interventions for customers.[204] Finally, Commissioner Price suggested reforms to require stronger verification and detection measures by telecommunications companies, including updates to account for the international calls and messages that scammers use to target Americans.[205]

Conclusion

Federal agencies have deployed a growing number of tools to combat overseas scam compounds and the transnational criminal organizations behind them — from criminal prosecutions, asset seizures, and sanctions to diplomatic engagement, victim outreach, and disruptions of the financial and technological infrastructure that enables fraud. These actions have produced

tangible results and demonstrate a growing recognition across the federal government of the scale and complexity of the scam threat.

At the same time, experts and officials have identified for the Committee necessary changes to strengthen the U.S. response. Scam networks operate across borders, jurisdictions, industries, and technologies, exploiting gaps between public and private sector entities. Meeting this challenge will require federal agencies to coordinate in a unified way; improve reporting and support for victims; work closely with the private sector to prevent and mitigate scam impacts; engage state and local officials; and ensure that laws and company practices evolve alongside the methods of transnational criminal organizations. As a first step, Congress must pass the ReportScams.Gov Act to mandate a unified federal strategy to combat scams and establish a central location for Americans to find information and assistance regarding scams.

In testimony before the Committee, FBI explained that the more than $17.7 billion in cyber scam losses that Americans reported to the Internet Crime Complaint Center last year equated to more than $2 million per hour.[206] Given the scale of these losses, Americans deserve urgent action from all parties with a role in preventing scams. No single action — or entity — will eliminate overseas scam compounds. But a more coordinated response that enables federal authorities to work with the private sector so that they can leverage businesses' information and technical capabilities could make it much harder and more costly for criminals overseas to victimize Americans.

---

[1] *See, e.g.*, Letter from Chairman David Schweikert, Vice Chairman Eric Schmitt, Ranking Member Maggie Hassan, and Rep. Don Beyer to Chairman Andrew N. Ferguson, Federal Trade Commission (Dec. 17, 2025).

[2] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[3] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Associate Counsel Richard Goldberg, Criminal Division, Department of Justice, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[4] *Satellite Images Reveal How Suspected Scam Compounds Appear Out of Nowhere*, WIRED (July 24, 2026) (www.wired.com/story/satellite-images-reveal-how-giant-scam-compounds-keep-on-expanding/); *see also Four Days to Make Victims Fall in Love: How Global Scammers Use US Tech to Fleece People*, AP (June 30, 2026) ("At least 25 new scam compounds have been built inside Myanmar since a high-profile crackdown along the Thai border last fall….").

[5] *Cambodia Says it Has Dismantled Scam Compounds, While Experts Call for Criminal Prosecutions*, AP (Sept. 23, 2026) (apnews.com/article/cambodia-scam-compounds-0b7365d65fa29e593cb9b01b53aec42a).

[6] U.S. Department of the Treasury: *Treasury Further Dismantles Overseas Scam Operations Targeting Americans* (June 23, 2026) (home.treasury.gov/news/press-releases/sb0538).

[7] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Deputy Assistant Director Gregory Heeb, Criminal Division, Federal Bureau of Investigation, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480); U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Associate Director Lois Greisman, Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480); U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Deputy Assistant Director Gregory Heeb, Criminal Division, Federal Bureau of Investigation, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[8] Letter from Paul D. Guaglianone, Bureau of Legislative Affairs, Department of State, to Chairman David Schweikert (May 14, 2026).

[9] Senate Foreign Relations Committee: *Ranking Member Shaheen, Senator Cornyn Introduce Bill to Counter Foreign Cyber Scams* (Oct. 1, 2025) (www.foreign.senate.gov/press/dem/release/ranking-member-shaheen-senator-cornyn-introduce-bill-to-counter-foreign-cyber-scams).

[10] Global Anti-Scam Alliance, *Global State of Scams Report 2025* (Oct. 7, 2025); *see also Online Scams May Already Be as Big a Scourge as Illegal Drugs*, The Economist (Feb. 6, 2025) (www.economist.com/briefing/2025/02/06/online-scams-may-already-be-as-big-a-scourge-as-illegal-drugs); *Compounding Misery: Myanmar's Scam Empire Gets Worse, Not Better*, The Economist (May 29, 2025) (www.economist.com/asia/2025/05/29/ myanmars-scam-empire-gets-worse-not-better).

[11] *See* Federal Trade Commission, *Protecting Older Consumers 2025-2026* (Oct. 19, 2026) (www.ftc.gov/system/files/ftc_gov/pdf/2026-older-adults-report-10192026.pdf).

[12] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Deputy Assistant Director Gregory Heeb, Criminal Division, Federal Bureau of Investigation, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[13] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Associate Director Lois Greisman, Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission, *Hearing on The Rising Global Scam Economy: Modernizing*

Federal Approaches to Protect Americans from Foreign Fraudsters, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[14] AP/Frontline, *Scammed* (Sept. 29, 2026) (www.pbs.org/wgbh/frontline/documentary/scammed/).

[15] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Associate Counsel Richard Goldberg, Criminal Division, Department of Justice, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480). *See also* AP/Frontline, *Scammed* (Sept. 29, 2026) (www.pbs.org/wgbh/frontline/documentary/scammed/).

[16] U.S. Attorney's Office for the District of Columbia: *Scam Center Strike Force Takes Major Actions Against Southeast Asian Scam Centers Targeting Americans* (Apr. 23, 2026) (www.justice.gov/usao-dc/pr/scam-center-strike-force-takes-major-actions-against-southeast-asian-scam-centers); U.S. Secret Service, Investment Fraud and Pig Butchering (www.secretservice.gov/investigations/investmentfraud-pigbutchering) (accessed Aug. 26, 2026).

[17] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Commissioner Reva Price, U.S.-China Economic and Security Review Commission, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[18] *Id.*

[19] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Deputy Assistant Director Gregory Heeb, Criminal Division, Federal Bureau of Investigation, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[20] U.S. Department of the Treasury: *Treasury Further Dismantles Overseas Scam Operations Targeting Americans* (June 23, 2026) (home.treasury.gov/news/press-releases/sb0538).

[21] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Karen P. Seifert, Scam Center Strike Force, U.S. Attorney's Office for the District of Columbia, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[22] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Associate Counsel Richard Goldberg, Criminal Division, Department of Justice, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480); U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Karen P. Seifert, Scam Center Strike Force, U.S. Attorney's Office for the District of Columbia, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[23] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Commissioner Reva Price, U.S.-China Economic and Security Review Commission, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[24] *Id.*

[25] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Karen P. Seifert, Scam Center Strike Force, U.S. Attorney's Office for the District of Columbia, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[26] *Id.*; U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[27] Exec. Order No. 14390, 91 Fed. Reg. 12051 (Mar. 6, 2026) (www.govinfo.gov/content/pkg/FR-2026-03-11/pdf/2026-04826.pdf).

[28] *Id.*

[29] *See, e.g.*, Letter from Chairman David Schweikert, Vice Chairman Eric Schmitt, Ranking Member Maggie Hassan, and Rep. Don Beyer to Chairman Andrew N. Ferguson, Federal Trade Commission (Dec. 17, 2025).

[30] *Id.*

[31] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[32] Senator Maggie Hassan: *Senators Hassan, Scott Introduce Bipartisan Bill to Establish ReportScams.Gov, First Central Portal for Americans to Report Scams and Get Help* (June 15, 2026) (www.hassan.senate.gov/news/press-releases/senators-hassan-scott-introduce-bipartisan-bill-to-establish-reportscamsgov-first-central-portal-for-americans-to-report-scams-and-get-help).

[33] *Id.*

[34] *Satellite Images Reveal How Suspected Scam Compounds Appear Out of Nowhere*, WIRED (July 24, 2026) (www.wired.com/story/satellite-images-reveal-how-giant-scam-compounds-keep-on-expanding/); *see also Four Days to Make Victims Fall in Love: How Global Scammers Use US Tech to Fleece People*, AP (June 30, 2026) ("At least 25 new scam compounds have been built inside Myanmar since a high-profile crackdown along the Thai border last fall….").

[35] Letter from Chairman Andrew N. Ferguson, Federal Trade Commission, to Ranking Member Maggie Hassan (Feb. 27, 2026).

[36] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Associate Director Lois Greisman, Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission, *Hearing on The Rising Global Scam Economy: Modernizing*

Federal Approaches to Protect Americans from Foreign Fraudsters, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[37] Letter from Chairman Andrew N. Ferguson, Federal Trade Commission, to Ranking Member Maggie Hassan (Feb. 27, 2026).

[38] *Id.*

[39] *Id.*

[40] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Associate Director Lois Greisman, Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[41] Federal Trade Commission: *FTC Ramps Up Fight to Close the Door on Illegal Robocalls Originating from Overseas Scammers and Imposters* (Apr. 11, 2023) (www.ftc.gov/news-events/news/press-releases/2023/04/ftc-ramps-fight-close-door-illegal-robocalls-originating-overseas-scammers-imposters).

[42] Letter from Chairman Andrew N. Ferguson, Federal Trade Commission, to Ranking Member Maggie Hassan (Feb. 27, 2026).

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] Federal Trade Commission, *Protecting Older Consumers 2024-2025* (Dec. 1, 2025) (www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf).

[48] Letter from Chairman Andrew N. Ferguson, Federal Trade Commission, to Ranking Member Maggie Hassan (Feb. 27, 2026).

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *Id.*; Federal Trade Commission, *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority* (July 2025) (www.ftc.gov/about-ftc/mission/enforcement-authority).

[56] Letter from Chairman Andrew N. Ferguson, Federal Trade Commission, to Ranking Member Maggie Hassan (Feb. 27, 2026).

[57] *Id.*; Federal Trade Commission: *FTC Reports Outline Efforts to Combat Cross-Border Fraud and Ransomware Attacks* (Oct. 20, 2023) (www.ftc.gov/news-events/news/press-releases/2023/10/ftc-reports-outline-efforts-combat-cross-border-fraud-ransomware-attacks).

[58] Federal Trade Commission, *The U.S. SAFE WEB Act and the FTC's Fight Against Cross-Border Fraud* (Oct. 20, 2023) (www.ftc.gov/system/files/ftc_gov/pdf/ftc_safe_web_congressional_report_oct_2023.pdf).

[59] *Id.*

[60] Letter from Chairman Andrew N. Ferguson, Federal Trade Commission, to Ranking Member Maggie Hassan (Feb. 27, 2026).

[61] Letter from Secretary Markwayne Mullin, Department of Homeland Security, to Chairman David Schweikert (June 10, 2026).

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] U.S. Immigration and Customs Enforcement: *ICE HSI Dismantles 'SIM Farms' in Nationwide Cyber Fraud Crackdown* (July 24, 2026) (www.ice.gov/news/releases/ice-hsi-dismantles-sim-farms-nationwide-cyber-fraud-crackdown).

[75] Letter from Secretary Markwayne Mullin, Department of Homeland Security, to Chairman David Schweikert (June 10, 2026).

[76] *Id.*

[77] *Id.*

[78] U.S. Immigration and Customs Enforcement: *ICE HSI Dismantles 'SIM Farms' in Nationwide Cyber Fraud Crackdown* (July 24, 2026) (www.ice.gov/news/releases/ice-hsi-dismantles-sim-farms-nationwide-cyber-fraud-crackdown).

[79] Letter from Secretary Markwayne Mullin, Department of Homeland Security, to Chairman David Schweikert (June 10, 2026); *see also* Federal Communications Commission, Avoid the Temptation of Smishing Scams (www.fcc.gov/avoid-temptation-smishing-scams) (accessed Aug. 26, 2026).

[80] Letter from Secretary Markwayne Mullin, Department of Homeland Security, to Chairman David Schweikert (June 10, 2026); *see also* Combatting Money Laundering in Cyber Crime Act of 2025 S. 1273, 119th Cong. (2025).

[81] Letter from Secretary Markwayne Mullin, Department of Homeland Security, to Chairman David Schweikert (June 10, 2026).

[82] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Karen P. Seifert, Scam Center Strike Force, U.S. Attorney's Office for the District of Columbia, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[83] *Id*.

[84] *Id*.

[85] *Id*.

[86] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Associate Counsel Richard Goldberg, Criminal Division, Department of Justice, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[87] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Karen P. Seifert, Scam Center Strike Force, U.S. Attorney's Office for the District of Columbia, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480); U.S. Attorney's Office for the District of Columbia, Scam Center Strike Force (www.justice.gov/usao-dc/scam-center-strike-force) (accessed Aug. 26, 2026); U.S. Attorney's Office for the District of Columbia: *Scam Center Strike Force Takes Major Actions Against Southeast Asian Scam Centers Targeting Americans* (Apr. 23, 2026) (www.justice.gov/opa/pr/scam-center-strike-force-takes-major-actions-against-southeast-asian-scam-centers-targeting).

[88] U.S. Attorney's Office for the District of Columbia: *Scam Center Strike Force Conducts Seizures of Chinese-Run Illicit Scammer Marketplace, and Restrains $52 Million in Laundered Crypto Scammer Funds In One Day* (Sept. 9, 2026) (www.justice.gov/usao-dc/pr/scam-center-strike-force-conducts-seizures-chinese-run-illicit-scammer-marketplace-and).

[89] U.S. Department of Justice: *Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes* (Oct. 14, 2025)

(www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged); U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Associate Counsel Richard Goldberg, Criminal Division, Department of Justice, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[90] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Karen P. Seifert, Scam Center Strike Force, U.S. Attorney's Office for the District of Columbia, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[91] U.S. Attorney's Office for the District of Columbia: *Scam Center Strike Force Announces Results of U.S. & Private Industry 'Disruption Week'* (June 3, 2026) (www.justice.gov/usao-dc/pr/scam-center-strike-force-announces-results-us-private-industry-disruption-week).

[92] *Id*.

[93] *Id*.

[94] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Deputy Assistant Director Gregory Heeb, Criminal Division, Federal Bureau of Investigation, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[95] *Id*.

[96] *Id*.

[97] *Id*.

[98] *Id*.

[99] *Id*.

[100] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Karen P. Seifert, Scam Center Strike Force, U.S. Attorney's Office for the District of Columbia, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480); U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[101] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[102] AP/Frontline, *Scammed* (Sept. 29, 2026) (www.pbs.org/wgbh/frontline/documentary/scammed/).

[103] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Karen P. Seifert, Scam Center Strike Force, U.S. Attorney's Office for the District of Columbia, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480)

[104] Letter from Paul D. Guaglianone, Bureau of Legislative Affairs, Department of State, to Chairman David Schweikert (May 14, 2026).

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] Email from U.S. Secret Service to Joint Economic Committee Minority Staff (Oct. 6, 2026).

[112] *Id.*

[113] Email from U.S. Secret Service to Joint Economic Committee Minority Staff (Apr. 23, 2026).

[114] Email from U.S. Secret Service to Joint Economic Committee Minority Staff (Aug. 12, 2026).

[115] *Id.*

[116] *CID Brings Back $3.62m Sent Abroad Thru' Fraud*, Daily Star (Mar. 29, 2026) (www.thedailystar.net/news/bangladesh/crime-justice/news/cid-brings-back-362m-sent-abroad-thru-fraud-4137926).

[117] Letter from Mosleh Uddin Ahmed, Additional Inspector General of Police, Chief of CID, Bangladesh Police, to Ambassador Brent T. Christensen (Apr. 2, 2026) (on file with the Committee – Minority).

[118] Letter from Paul D. Guaglianone, Bureau of Legislative Affairs, Department of State, to Chairman David Schweikert (May 14, 2026).

[119] *Id.*

[120] *Id.*; U.S. Mission to ASEAN, *10 Public-Private Partnership Principles for Tackling Online Scams* (Jan. 17, 2026) (asean.usmission.gov/10-public-private-partnership-principles-for-tackling-online-scams/).

[121] Letter from Paul D. Guaglianone, Bureau of Legislative Affairs, Department of State, to Chairman David Schweikert (May 14, 2026).

[122] *Id.*

[123] *Id.*

[124] Letter from Acting Principal Deputy Assistant Secretary Mason Champion, Office of Legislative Affairs, Department of the Treasury, to Ranking Member Maggie Hassan (Jan. 22, 2026).

[125] Email from Christopher Burdick, Deputy Assistant Secretary, Office of Legislative Affairs, to Joint Economic Committee Minority Staff (Oct. 7, 2026).

[126] Financial Crimes Enforcement Network, *FinCEN Alert on Money Laundering Activity Associated with Digital Asset Investment Scam Centers* (Sept. 3, 2026) (www.fincen.gov/system/files/2026-08/FinCEN-Alert-Scam-Centers.pdf); Financial Crimes Enforcement Network, *Digital Asset Investment Scams: 2023-2025 Threat Pattern & Trend Information* (Sept. 2026) (www.fincen.gov/system/files/2026-08/FinCEN-FTA-Digital-Asset-Investment-Scams.pdf).

[127] Financial Crimes Enforcement Network, *Digital Asset Investment Scams: 2023-2025 Threat Pattern & Trend Information* (Sept. 2026) (www.fincen.gov/system/files/2026-08/FinCEN-FTA-Digital-Asset-Investment-Scams.pdf).

[128] Letter from Acting Principal Deputy Assistant Secretary Mason Champion, Office of Legislative Affairs, Department of the Treasury, to Ranking Member Maggie Hassan (Jan. 22, 2026).

[129] Financial Crimes Enforcement Network: *FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System* (Oct. 14, 2025) (www.fincen.gov/news/news-releases/fincen-issues-final-rule-severing-huione-group-us-financial-system); Financial Crimes Enforcement Network: *FinCEN Proposes to Sever H-Pay Service PLC and Other Huione Group Successor Entities from the U.S. Financial System* (June 23, 2026) (www.fincen.gov/news/news-releases/fincen-issues-final-rule-severing-huione-group-us-financial-system).

[130] Financial Crimes Enforcement Network, *FinCEN Rapid Response Program Fact Sheet* (Apr. 15, 2026) (www.fincen.gov/system/files/2026-04/RRPFactSheet.pdf).

[131] *Id.*

[132] Financial Crimes Enforcement Network: *FinCEN's Rapid Response Program Interdicts Nearly $2 Billion on Behalf of U.S. Cyber-Enabled Fraud Victims* (Apr. 15, 2026) (www.fincen.gov/news/news-releases/fincens-rapid-response-program-interdicts-nearly-2-billion-behalf-us-cyber); Financial Crimes Enforcement Network, *FinCEN Rapid Response Program Fact Sheet* (Apr. 15, 2026) (www.fincen.gov/system/files/2026-04/RRPFactSheet.pdf).

[133] Letter from Acting Principal Deputy Assistant Secretary Mason Champion, Office of Legislative Affairs, Department of the Treasury, to Ranking Member Maggie Hassan (Jan. 22, 2026).

[134] *Id.*

[135] Senate Committee on Finance, *Hearing on Nominations*, 119th Cong. (July 16, 2026) (S. Hrg. 119-480).

[136] G20 Chair's Statement: *Second Meeting of G20 Finance Ministers and Central Bank Governors, Asheville, United States of America* (Sept. 1, 2026) (home.treasury.gov/news/press-releases/sb0620).

[137] Letter from Acting Principal Deputy Assistant Secretary Mason Champion, Office of Legislative Affairs, Department of the Treasury, to Ranking Member Maggie Hassan (Jan. 22, 2026).

[138] Email from Christopher Burdick, Deputy Assistant Secretary, Office of Legislative Affairs, to Joint Economic Committee Minority Staff (Oct. 7, 2026).

[139] U.S. Department of the Treasury: *Treasury Sanctions Cambodian Senator Kok An and Scam Center Network Defrauding Americans* (Apr. 23, 2026) (home.treasury.gov/news/press-releases/sb0469).

[140] *Id.*

[141] U.S. Department of the Treasury: *Treasury Further Dismantles Overseas Scam Operations Targeting Americans* (June 23, 2026) (home.treasury.gov/news/press-releases/sb0538).

[142] U.S. Department of the Treasury: *Treasury Cracks Down on Transnational Criminal Organization Behind Cyber Scam Operations Targeting Americans* (Sept. 9, 2026) (home.treasury.gov/news/press-releases/sb0624).

[143] *Id.*

[144] Exec. Order No. 14390, 91 Fed. Reg. 12051 (Mar. 6, 2026) (www.govinfo.gov/content/pkg/FR-2026-03-11/pdf/2026-04826.pdf).

[145] *Id.*; U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Associate Counsel Richard Goldberg, Criminal Division, Department of Justice, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480). In August 2026, a presidential memorandum expanded on this framework by allowing vetted U.S. companies to conduct offensive and surveillance cyber operations against transnational criminal organizations under federal direction, authorization, and oversight. President Donald J. Trump, *Presidential Memorandum: Expanding Capabilities to Combat Transnational Cyber-Enabled Crime* (Aug. 12, 2026) (www.whitehouse.gov/presidential-actions/2026/08/expanding-capabilities-to-combat-transnational-cyber-enabled-crime/).

[146] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Kate Griffin, Inclusive Finance, The Aspen Institute Financial Security Program, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[147] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Seto J. Bagdoyan, Forensic Audits and Investigative Service, U.S. Government Accountability Office, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[148] *Id.*

[149] *Id.*

[150] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[151] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Kate Griffin, Inclusive Finance, The Aspen Institute Financial Security Program, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[152] *Id.*

[153] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[154] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Seto J. Bagdoyan, Forensic Audits and Investigative Service, U.S. Government Accountability Office, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[155] *Id.*

[156] *Id.*

[157] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[158] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Seto J. Bagdoyan, Forensic Audits and Investigative Service, U.S. Government Accountability Office, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[159] Government Accountability Office, *Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams* (GAO-25-107088) (Apr. 2025) (www.gao.gov/assets/gao-25-107088.pdf); U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Seto J. Bagdoyan, Forensic Audits and Investigative Service, U.S. Government Accountability Office, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[160] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Senior Director Kathy Stokes, Fraud Prevention Programs, AARP Fraud Watch Network, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[161] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[162] *Id.*

[163] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Kate Griffin, Inclusive Finance, The Aspen Institute Financial Security Program, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[164] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Senior Director Kathy Stokes, Fraud Prevention Programs, AARP Fraud Watch Network, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[165] *Id.*

[166] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[167] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Kate Griffin, Inclusive Finance, The Aspen Institute Financial Security Program, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[168] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Commissioner Reva Price, U.S.-China Economic and Security Review Commission, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[169] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[170] *Id.*

[171] *Id.*

[172] *Id.*

[173] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Kate Griffin, Inclusive Finance, The Aspen Institute Financial Security Program, *Hearing*

on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[174] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[175] *Id*.

[176] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Commissioner Reva Price, U.S.-China Economic and Security Review Commission, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[177] *Id*.

[178] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[179] Records on file with the Committee – Minority.

[180] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[181] *Id*.

[182] *Id*.

[183] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Commissioner Reva Price, U.S.-China Economic and Security Review Commission, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[184] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Kate Griffin, Inclusive Finance, The Aspen Institute Financial Security Program, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[185] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Seto J. Bagdoyan, Forensic Audits and Investigative Service, U.S. Government Accountability Office, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480); U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[186] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[187] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Seto J. Bagdoyan, Forensic Audits and Investigative Service, U.S. Government Accountability Office, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[188] *Id.*

[189] *Id.*

[190] Letter from Chairman Andrew N. Ferguson, Federal Trade Commission, to Ranking Member Maggie Hassan (Feb. 27, 2026).

[191] Letter from Secretary Markwayne Mullin, Department of Homeland Security, to Chairman David Schweikert (June 10, 2026).

[192] Letter from Paul D. Guaglianone, Bureau of Legislative Affairs, Department of State, to Chairman David Schweikert (May 14, 2026).

[193] *Id.*

[194] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Karen P. Seifert, Scam Center Strike Force, U.S. Attorney's Office for the District of Columbia, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480); U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[195] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Kate Griffin, Inclusive Finance, The Aspen Institute Financial Security Program, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[196] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Senior Director Kathy Stokes, Fraud Prevention Programs, AARP Fraud Watch Network, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[197] *Id.*; *see also* U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Kate Griffin, Inclusive Finance, The Aspen Institute Financial Security Program, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480) ("Provide relief to victims by eliminating or reducing tax penalties on early withdrawal of 401(k) funds sent to a scammer.").

[198] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Commissioner Reva Price, U.S.-China Economic and Security Review Commission, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[199] *Id.*

[200] U.S. Congress Joint Economic Committee, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[201] *Id.*

[202] *Id.*

[203] *Id.*

[204] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Director Kate Griffin, Inclusive Finance, The Aspen Institute Financial Security Program, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[205] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Commissioner Reva Price, U.S.-China Economic and Security Review Commission, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).

[206] U.S. Congress Joint Economic Committee, Testimony Submitted for the Record of Deputy Assistant Director Gregory Heeb, Criminal Division, Federal Bureau of Investigation, *Hearing on The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (S. Hrg. 119-480).