S. HRG. 119–303

MADE IN CHINA, PAID BY SENIORS: STOPPING THE SURGE OF INTERNATIONAL SCAMS

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING

UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

SECOND SESSION

WASHINGTON, DC

JANUARY 14, 2026

Serial No. 119–22

Printed for the use of the Special Committee on Aging

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

62–924 PDF WASHINGTON : 2026

SPECIAL COMMITTEE ON AGING

RICK SCOTT, Florida, *Chairman*

DAVE McCORMICK, Pennsylvania
JIM JUSTICE, West Virginia
TOMMY TUBERVILLE, Alabama
RON JOHNSON, Wisconsin
ASHLEY MOODY, Florida
JON HUSTED, Ohio

KIRSTEN E. GILLIBRAND, New York
ELIZABETH WARREN, Massachusetts
MARK KELLY, Arizona
RAPHAEL WARNOCK, Georgia
ANDY KIM, New Jersey
ANGELA ALSOBROOKS, Maryland

MCKINLEY LEWIS, *Majority Staff Director*
CLAIRE DESCAMPS, *Minority Staff Director*

C O N T E N T S

MADE IN CHINA, PAID BY SENIORS: STOPPING THE SURGE OF INTERNATIONAL SCAMS

Wednesday, January 14, 2026

U.S. SENATE
SPECIAL COMMITTEE ON AGING
Washington, DC.

The Committee met, pursuant to notice, at 3:32 p.m., Room 216, Hart Senate Office Building, Hon. Rick Scott, Chairman of the Committee, presiding.

Present: Senator Scott, Johnson, Moody, Gillibrand, and Warren.

OPENING STATEMENT OF SENATOR RICK SCOTT, CHAIRMAN

The CHAIRMAN. The U.S. Senate Special Committee on Aging will now come to order. Today, we're here to discuss a growing threat to American seniors and our families. The surge of international scams rooted in Communist China and its regional criminal networks. Scams targeting seniors are stealing billions of dollars from hardworking Americans, and we here in Congress have a responsibility to confront them head on.

The scope of this problem is staggering. In 2024, older Americans lost more than $4.8 billion to fraud according to the FBI. These are retirees who spend decades working, saving, and planning for their futures, only to have their lives upended by monsters operating criminal networks overseas.

As our Committee reports, age of fraud makes clear these are not small-time criminals. These are highly organized transnational enterprises, many of them directed or enabled by the Chinese Communist Party. We know how these groups work. They rely on Chinese platforms, Chinese payment channels, and scam compounds in Myanmar, Cambodia, Laos, and elsewhere, compounds built and staffed by trafficked workers forced to carry out scams, targeting our friends Americans.

Not only is this a disgusting display of our national failures to protect human rights, dignity, and security, it's also another way Communist China is undermining our country and targeting the American people. Beijing has allowed this criminal infrastructure to grow and thrive. No matter what you believe; indifference, lack of enforcement, or strategic tolerance, Communist China is the epicenter of the global scam industry that drains American savings and destabilizes families.

I decided to make this the first hearing of the year to send a clear message that we will not tolerate any further inaction as the CCP seeks to hurt our seniors in what should be their golden years. Communist China and criminal enterprise network must be stopped. We have common-sense legislation ready to go that would make a real difference in combating scams and holding those responsible accountable.

At the end of last year, Ranking Member Gillibrand and I, along with our fellow committee members, Senators Ashley Moody and Mark Kelly, introduced the National Strategy for Combating Scams Act. This bill would finally require a coordinated whole-of-government response to fight fraud, recognizing that after billions upon billions of dollars are being lost every year, it's time we finally get federal, state, and private sector partners together under a unified strategy.

I'm also proud that my Scam Compound Accountability and Mobilization, or SCAM Act, was passed by the Senate last month. This bill would give the Treasury Department the authority to sanction scam compounds and the criminal networks behind them. Criminals shouldn't be free to hide behind foreign compounds, use Chinese infrastructure, and still access the U.S. financial system.

Additionally, Ranking Member Gillibrand and I are also pushing for the GUARD Act. This bill strengthens penalties against criminals who target older Americans, and gives law enforcement more tools to prevent these crimes.

These three bills are bipartisan, they're common-sense, and they're designed to protect the American people. It's time we all come together and get this legislation passed so we can stop the bleeding of American dollars to international criminals.

Here's the reality: There isn't a person alive who isn't susceptible to Communist China scams. They won't stop unless we do something. We cannot continue to sit idly by as these criminals harm Americans. Now is the time to take action to protect our seniors and every American.

I look forward to a productive discussion today with our witnesses, and now I'd like to recognize Ranking Member Gillibrand for opening statement.

OPENING STATEMENT OF SENATOR KIRSTEN E. GILLIBRAND, RANKING MEMBER

Senator GILLIBRAND. Thank you, Chairman Scott, and thanks for calling today's hearing. Welcome, witnesses. I appreciate you all being here today.

In recent years, scams targeting older adults have grown more sophisticated and widespread because of the rise of scam centers. These centers are fueled by the labor of human trafficking victims, new developments in technology, and the use of cryptocurrency. Older Americans everywhere are vulnerable to the rise of these scams, including my own constituents.

For example, a senior in Jefferson County, New York, was convinced through a romance scam to withdraw most of his 401(k) funds and transfer the money into cryptocurrency. That is a loss that stings. It can derail retirement plans, pull apart families, and subject seniors to emotional and material harm. Unfortunately, vic-

tims can struggle to report scams due to stigma and shame. Some communities may face additional barriers related to language or fear.

This hearing focuses on transnational scams that are facilitated by Chinese criminal organizations. It is worth remembering that Asian immigrants, including many Chinese Americans, can be preferred targets for transnational scammers because of a common language and culture, as well as their familial ties to China.

We must remember that international scams are worldwide, and this phenomenon requires robust and coordinated prevention, enforcement, and protection efforts. One positive development has taken place in New York. The state's Department of Aging, the Association on Aging in New York, and the Silver Shield Partnership empower older New Yorkers with tools that allow them to instantly perform scam checks via email, text, and online to report scams to the FBI and the FTC in one click.

However, there is still much more work to be done. Last year, the Government Accountability Office published a report on federal efforts to combat scams. GAO noted an alarming lack of coordination amongst federal agencies. Based on recommendations from GAO's report, I introduced the National Strategy for Combating Scams Act with Chairman Rick Scott, and Senators Mark Kelly, and Ashley Moody. Our legislation would require the FBI to lead a multi-agency working group to create a national strategy to combat scams.

Last July, I introduced the bipartisan Guarding Unprotected Aging Retirees from Deception, or GUARD Act, with Senator Katie Britt and Chairman Scott. The GUARD Act will increase resources for law enforcement to utilize blockchain technology for investigating financial fraud.

I appreciate the willingness of my colleagues to work with me on legislation to combat scams, and I look forward to our discussion today. Thank you.

The CHAIRMAN. Thank you, Ranking Member.

I'd like to welcome our expert witnesses who are here to talk about how serious this issue is, and the steps we can take to protect our seniors. First, I'd like to introduce Nathan Picarsic, Senior Fellow at the Foundation for Defensive Democracies. He's a leading expert on Communist China's global economic and strategic ambitions, with more than a decade of experience analyzing how the CCP weaponizes technology, economic leverage, and military/civil fusion to expand its influence.

He was the first Western analyst to document Beijing's China Standards 2035 plan. His insights grounded in primary source research have informed policymakers and appear in major publications including The Wall Street Journal, The Washington Post, Bloomberg, and CNBC.

Thank you for being here. Please begin your testimony.

STATEMENT OF NATHAN PICARSIC, SENIOR FELLOW, THE FOUNDATION FOR DEFENSE OF DEMOCRACIES, WASHINGTON, DC

Mr. PICARSIC. Thank you, Chairman Scott, Ranking Member Gillibrand, and committee members, for the opportunity to offer testimony alongside my esteemed co witnesses.

As Senator Scott noted, international scams targeting elderly populations in America already account for billions of dollars of harm annually. Chinese-linked operations play an outsized role in executing and supporting these scams, and as testimony, I hope to convey three points.

State-backed scam operations support China's broader approach to great power competition. The Chinese government plays a role in the proliferation of international scams and last, there's opportunity for the Federal Government to lead and empower coordination that can disrupt and deter Chinese state-backed scams.

International scams are directly relevant to strategic competition. Social cohesion is a pivotal battleground. Defending against external attacks on our vulnerable, including our elderly, is a fundamental requirement for succeeding in long-term peacetime competition. China understands this, and China deliberately positions foment, fissures within American society, and to tease at American vulnerabilities.

We know and talk a lot about China's state-backed hacking, industrial espionage, foreign information campaigns. Those create national security risks for the United States by activating a united front that subverts markets captures elites and does the bidding of the Chinese State through obscured and direct channels.

The same Chinese campaign also enables the transnational criminal forces that execute and redeem profits from elder scams in the United States. There's growing awareness of China's leading role as evidenced by this hearing, but recognition of the full scope of this threat lags, so too does marshaling a right-sized response, one they impose of the Chinese government for its role and deter attacks on America's elderly moving forward.

State-backed scam has emerged from China, just like state-backed industrial espionage efforts. China plays a leading role in scams that originate both in China itself and outside in hotspots across southeast Asia, for example, where scam operations exist and scam compounds operate under Chinese leadership.

China's criminal networks are permitted, and at times, abetted by the Chinese State in its ruling Communist Party. The leaders of the Chinese Communist Party would much rather see criminal acts perpetrated against foreign targets than against China's own aging population. Accordingly, the Chinese government has allowed China's cottage industry of scam operations, including those to target elder victims to exist and to excel.

China's criminal networks offer several fundamental advantages. First, China's criminal networks benefit from advanced technology. Second, China's banking and sector has globalized, allowing China's criminal networks to transfer money across borders, obfuscate the flow of funds, and evade regulatory authorities. Those advantages fuel Chinese criminal underground that is already global.

Elder scams is a key revenue source for their broader criminal ecosystem, and Chinese criminal networks lead the way in refining tactics. Pig butchering, for example, has emerged as a term to describe cyber-enabled scams that frequently drain elderly victims of their savings over a sequence of courtship and scamming.

The practice of pig butchering and its dehumanizing framing originated in China. The term was first coined in Chinese. The

power of the Chinese financial system compounds the threat posed by those Chinese tactics and by the Chinese perpetrators.

The problem isn't just that there's an internationalized Chinese banking system. The problem is that the Chinese State makes it nearly impossible to reclaim stolen funds. Victims often have little recourse after funds have been offshore. The systemic nature of China's state-backed scamming amounts to great power stakes.

The United States cannot afford to stand by as Chinese criminal networks deplete American social trust and the bank accounts of countless Americans. A whack-a-mole response will not solve this challenge. State-backed scam networks can outfox their targets and the authorities that are invariably playing catch up.

To offset this imbalance, the United States needs to erect protections and increase sensing, invest in coordination between local, federal, and private sector forces, and enforce aggressively against Chinese criminal networks in the arms of the Chinese State, including its financial apparatus that support them to be able to send a clear deterrent signal to Beijing.

Americans should not be surprised by the Chinese government whatsoever. This is the same international actor that decimated global public health through their negligence with COVID–19, the same actor that hacks the U.S. Government and critical infrastructure that maliciously fuels the fentanyl crisis ravaging America's heartland, and is building a military to challenge the United States and to bully America's allies and partners.

This is not a responsible stakeholder. This is an adversary. We should take no pride in treating China with kid gloves, or endlessly hoping that they'll mature into a responsible actor and worse yet, the state-backed scamming that they propel proves that China is an enemy keen to target our vulnerable populations. America needs to respond forcefully to protect our elders, to support our social fabric as well as our chances in long-term competition.

Thank you again for the opportunity to contribute to this hearing and for the work of the Committee to protect America's aging population.

The CHAIRMAN. Thank you. Next, I'd like to recognize Kathy Stokes, Senior Director of Fraud Prevention within the Fraud Watch Network at AARP. It's nice to see you again. Ms. Stokes is one of the Nation's leading experts on financial exploitation targeting older adults, and she has spent years studying the tactics criminals use, the vulnerabilities they exploit, and the long-term impact fraud has on seniors and their families.

This Committee has welcomed AARP several times over the years. I just want to take a second and say thank you for your organization's leadership in this space. Helping educate your members helps millions of Americans stay up to date on the latest fraud trends and saves innumerable amounts of money.

Thank you for being here and please begin your testimony.

STATEMENT OF KATHY STOKES, SENIOR DIRECTOR, FRAUD PREVENTION PROGRAMS, AARP, WASHINGTON, DC

Ms. STOKES. Thank you, Chairman Scott, for inviting me to testify, and I want to express my appreciation to you Ranking Mem-

ber Gillibrand and all of the Committee members for holding this timely and important hearing.

My name is Kathy Stokes, Senior Director of Fraud Prevention Programs, AARP Fraud Watch Network. I'm here on behalf of AARP, and we represent 125 million Americans, aged 50 and older, and their families, and we deeply appreciate your attention to the surge of international scams that are targeting our seniors.

Now, fraud is a national crisis but bigger than most of us recognize. The Federal Trade Commission reported $12.8 billion stolen in 2024, but the true cost is far, far higher. They went back to that $12.8 billion and revised it in December to $196 billion leaving our economy in a single year to fraud, $81 billion of that from our Nation's seniors. They robbed victims of savings, of independence and security.

Now, the Fraud Watch Network is on the front lines of educating millions of consumers supporting victims and driving systemic change. Our helpline receives 500 calls a day from those reporting scams, to victims seeking help, and we also offer support groups to help victims rebuild their lives.

We hear from people like Lori, an oncology account specialist for a pharmaceutical company. A few years ago, she fell in love with a man whom she first met when he reached out to her on LinkedIn to ask for advice about moving to her area. He then spent months carefully grooming her.

As her caring and trust deepened, he asked for Lori's help. She ended up loaning him $675,000, nearly all of her savings, including funds from her 401(k) plan and loans and of course, when she finally discovered it was a scam, she was devastated and then, she learned that she'd have to pay $225,000 in federal taxes on the money that was stolen that she no longer has. The massive tax bill forced Lori to file for bankruptcy, and the IRS was first in line for payment.

In addition to fraud prevention through education, AARP is leading an effort to change how we talk about and think about fraud victims. Our Words Matter campaign shows that blaming victims deprioritizes fraud as a crime, and we're seeing real movement among consumers, media, industry, policymakers toward understanding that fraud is a crime and it's not the victim's fault.

AARP is also proud to be a founder of the National Elder Fraud Coordination Center, which aggregates intelligence related to elder fraud, to support law enforcement and NEFCC recently revived a stalled transnational federal fraud investigation when it was able to identify a network of 24 U.S.-based shell companies receiving victim funds. Indeed, transnational criminal organizations drive the expansion and the funds they amass represent a national security threat.

In the sophisticated scam we've already talked about originating in Southeast Asia, these Chinese organized crime rings are using human trafficking for frontline scammers targeting and devastating Americans, forcing many to rely on government safety nets in their retirement.

We're pleased to see solutions proposed by Congress, including the introduction of the GUARD Act and the National Strategy for Combating Scams Act by the chair, and ranking member, and other

Senators. These bills seek to improve the state and local response to fraud, and better coordinate agency efforts, and ensure law enforcement has the tools needed to combat these crimes.

We also advocate for reinstating the personal casualty and theft loss deduction as the tax relief for Victims of Crimes, Scams, and Disasters Act would do. Victims like Lori who end up owing taxes on stolen funds, they no longer end up stuck with a bill that they don't deserve and have no way to pay. Essentially, they're being revictimized by the Federal Government.

There is no single solution and every sector has a role to play. Individuals can certainly take steps to protect themselves and their loved ones. Industry must innovate on fraud controls. Tech companies and telcos must build security into products so they're secure by design and safe by default and the financial services industry must do its part to stop their customers from being defrauded.

Addressing fraud does require a whole-of-society response. We can't educate, or engineer, or regulate, or arrest our way out of this crisis alone but altogether, we can disrupt the fraud business model, protect millions of Americans, and safeguard our economy.

Thank you for your leadership and commitment to protecting older Americans, and I look forward to your questions.

The CHAIRMAN. She never met him, right? It was just all online.

Ms. STOKES. Well, they had video. Yes.

Senator GILLIBRAND. Oh, he had video chats?

Ms. STOKES. Oh, yes. He was no stranger in that sense. Yes.

The CHAIRMAN. I wonder if it was really him.

Ms. STOKES. Oh, it was probably transnational criminal organization and they were using deepfake.

The CHAIRMAN. Yes. All right. Now, I'd like to recognize and introduce Jacqueline Burns Koven, Head of Cyber Threat Intelligence at Chainalysis. Ms. Koven leads the company's analysis of cyber-enabled crime, including cryptocurrencies, scams, ransomware, and transactional fraud networks targeting victims in the United States.

Her work focuses on tracking illicit financial flows, and identifying how overseas criminal organizations, including China-linked networks, move and launder stolen funds through digital assets. She regularly supports U.S. law enforcement policymakers with data-driven insights that help disrupt scam operations that recover stolen funds.

Thank you for being here.

STATEMENT OF JACQUELINE BURNS KOVEN, HEAD OF CYBER THREAT INTELLIGENCE, CHAINALYSIS, NEW YORK, NEW YORK

Ms. BURNS KOVEN. Thank you, Chairman Scott, Ranking Member Gillibrand, and distinguished members of the Special Committee. Thank you for inviting me to testify on the pressing issue of international scams targeting older Americans as an urgent matter of national security.

My name is Jacqueline Burns Koven, and I'm the head of Cyber Threat Intelligence for the blockchain data platform Chainalysis where we harness the transparency of blockchain so that banks, businesses, and governments have the data, and investigations,

compliance, and security solutions they need for this new digital economy to thrive.

We track cryptocurrency used by illicit actors such as those carrying out investment and impersonation scams and provide data on their financial activity to private and public sector customers include, including the Federal Government.

Through Chainalysis' unique visibility into the crypto economy and illicit fund flows, we see how seemingly small scam payments from individual victims are pooled and funneled into industrial scale fraud conglomerates. We know that behind these transactions, are real people, often seniors who are being manipulated into sending their life savings through technologies they may not fully understand.

These scam syndicates are incredibly well-resourced. According to Chainalysis data, 2025 was a record year for scammers stealing an estimated $17 billion in cryptocurrency. Chinese scam conglomerates are undeniably the global market leaders in fraud, in large part to their abuse of innovations, including crypto and AI, to make their schemes more convincing and scalable.

Everything from social media profiles, mass calling and SMS spamming tools, deepfake, and voice cloning, to laundering is available in Chinese language underground marketplaces, and they leverage cryptocurrency as a form of payment. Cryptocurrencies are often the financial rails of choice for scammers for the same reasons legitimate users use them. Transactions are cross-border and instantaneous.

I'm here today to emphasize that fraudsters use of cryptocurrency should place them at a fundamental disadvantage given the traceability and feasibility of many of these assets. At Chainalysis, we analyze transaction data from the blockchain networks to provide clear information into scam networks and laundering at a level of transparency that isn't possible in traditional forms of value transfer.

Blockchain intelligence should be considered foundational for understanding the fraud problem at both strategic and tactical levels. Law enforcement and regulatory bodies can disrupt these networks, cut them off from the global financial institutions and make it harder for them to profit by targeting illicit entities and networks on the blockchain with sanctions and asset seizure.

Blockchain analytics offers unique opportunities to trace proceeds of crime, identify additional victims, and partner with the private sector to disrupt illicit networks and pursue restitution rather than relying on one-off criminal investigations.

However, despite this huge potential for disruption, scammers are exploiting the disjointed and reactive nature of how public and private sectors respond to their schemes. This crisis requires a unified and technology-enabled response preventing Americans from engaging with scams altogether, and identifying and dismantling enterprises responsible for perpetrating scams.

As such, my recommendations include, first, the creation of a national counter scam strategy, orchestrating a comprehensive response, including centralizing scam reporting, streamlining coordinated action to dismantle scam conglomerates, and return funds to

victims in facilitating information sharing between the public and private sectors.

Today's scam victims have multiple agencies they can report to, yet, there's no easy mechanism for these agencies to share with each other or the private sector of what whose best positioned to prevent for additional victims. We need a coordinated approach using all levers of government to target the scam ecosystem holistically from the money launderers, to the fishing kit developers, and data brokers.

Second, we need to leverage advanced technologies to combat scammers' growing sophistication. Too often, scam victims are turned away from authorities who are ill-equipped to properly assist crypto cases. This challenge also demands a paradigm shift from reactive enforcement to proactive disruption through AI-powered fraud prevention technology to identify scammers before they meet their victims, and empower law enforcement to move decisively upstream and take the fight directly to scammers.

Third, we need to provide financial institutions with guidance to help them intervene when customers attempt to send funds to scams. Clear consistent guidelines could help firms navigate when and how they can slow-block, scrutinize scam transactions and what form of friction are appropriate without overreaching.

Last, we need to close gaps in AML/CFT standards implementation, especially countries that host services scammers rely on to launder funds defrauded from Americans and in the absence of cooperation, more pressure is needed to disrupt the offshore financial networks and the digital asset services flagrantly abusing laws and regulatory norms.

Once again, thank you for the opportunity to provide testimony on this important topic, and continue to be a helpful partner on initiatives by Congress to better protect Americans, especially the most vulnerable. I look forward to your questions.

The CHAIRMAN. Thank you. Now, I'd like to recognize Ranking Member Gillibrand to introduce the next witness.

Senator GILLIBRAND. Thank you, Mr. Chairman. I want to move to introduce Seto Bagdoyan. Mr. Bagdoyan is Director for Audit Services at The Government Accountability Office's Forensic Audits and Investigative Service mission team.

Mr. Bagdoyan previously served in a variety of positions at GAO, including as an advisor in GAO's Office of congressional Relations, and as Assistant Director for Homeland Security and Justice. He's also served as an congressional detail with the Senate Finance Committee, and the House Committee on Homeland Security, and in private consultancy positions focusing on political risk and homeland security.

Mr. Bagdoyan, you may begin your testimony.

STATEMENT OF SETO BAGDOYAN, DIRECTOR, AUDIT SERVICES, FORENSIC AUDITS & INVESTIGATIVE SERVICE, GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, DC

Mr. BAGDOYAN. Thank you, Chairman Scott, Ranking Member Gillibrand, Senator Johnson. I'm pleased to discuss today GAO's April 2025 report about scams targeting consumers, including older adults and the federal response.

Scams are a method of committing fraud by employing deception or manipulation enabled by technology such as AI to achieve financial gain. They involve scammers, often operating from foreign countries, as we've heard today, engaging targeted victims with a type of scam and requesting payment under false purposes.

One example highlights the scope and reach of scams and their financial toll on consumers. A 2023 international police operation against online financial crime, including scams, yielded over 3,000 arrests and seizures of $300 million in assets across 34 countries, including the United States.

However, the full extent of losses and the risks that underpin them is elusive, since these estimates often are based on under-reported consumer complaints rather than systematic assessments of scam risks and their financial and other implications.

In our report, we noted that given the scope, scale, and nature of scams and the risks they pose, the federal response falls short on risk management fundamentals. Especially, it lacks a governmentwide strategy and a lead agency to organize, coordinate, and target multiple activities by individual agencies.

Importantly, and this is very important, there is no common definition of what constitutes a scam, and no systematic assessment of scams and the risks they pose to consumers. Accordingly, there's no assurance that the federal response as it is now - is addressing the right risks and the right priorities in the right manner.

A government-wide strategy would introduce risk management fundamentals to help ensure that the federal response to a significant, dynamic, and sophisticated risk is integrated, prioritized, targeted, and adaptable. We made 16 recommendations to FBI, FTC, and CFPB, the federal agencies best positioned to lead the federal response.

To date, these agencies' responses are mixed. They've agreed with some recommendations and disagreed with, or took no explicit positions on, others. For example, FBI agreed to assume the lead for the governmentwide strategy and outlined related initial steps. However, its disagreement with other recommendations essential for an effective strategy, such as adopting a common definition, is concerning.

While we acknowledge agencies' positions on these challenging undertakings, it's imperative for them to implement all recommendations. Otherwise, the governmentwide strategy will ultimately be ineffective.

In closing, scams, including those of foreign origin, pose immediate risks of harm to consumers. Accordingly, these risks require a decisive, expeditious federal response. The response is underpinned by adopting a common definition of scams.

This serves as the organizing principle for assessing and quantifying the risks posed by scams, and crafting and implementing a governmentwide strategy to counter them, including those of foreign origin. In this regard, legislative actions such as S. 3355 would charge the federal response, and importantly, establish oversight and ensure accountability.

Chairman Scott, this concludes my remarks. I welcome the Committee's questions. Thank you.

The CHAIRMAN. Thanks for coming, and thanks for your testimony. Now, we'll go to the questions. Senator Johnson, if you want to start us off.

Senator JOHNSON. Thank you, Mr. Chairman. Ms. Stokes, being the accountant here, you caught my attention when we talked about, is it Lori? She emptied what, her 401(k) account, or whatever, $600,000-and-some?

Ms. STOKES. Yes. It was primarily from her 401(k).

Senator JOHNSON. How in the world did she have a greater than $200,000 tax liability? I mean, was it gift tax, or was it, you know, 10 percent early withdrawal from—I mean, I don't understand how the tax penalty could be that high

Ms. STOKES. I'm not an accountant, so I don't know. I just know that it was $225,000, and that was what forced her to file Chapter 13.

Senator JOHNSON. I would ask you to go back to Lori. I'd like to get the details because that makes no sense. I mean, if they considered she shouldn't have had to pay anything, I can maybe see a penalty for earlier withdrawal, but that'd be cruel.

I mean, she made a loan and she lost her money. If anything, she'd get a tax refund on something like that. It literally makes no sense to me. I'd really appreciate that.

Ms. STOKES. Absolutely.

Senator JOHNSON. In a number of testimonies, you have laid out some of these scams, but we didn't really, other than Lori's romantic scam. I'm just asking each of you, what is it? What's the hook? Can you give anybody watching this, you know, be aware when you see this.

I'll start with Mr. Picarsic. I mean, what are the two or three most common hooks? I'll just go right down the line.

Mr. PICARSIC. Yes. I mean, I think the pig butchering, which is similar to the Lori attack sort of confidence scheme, and recurring outreach from an actor that you're unfamiliar with or that is showing some sort of romantic or unprompted solicitation.

Senator JOHNSON. You'd say that the romantic one is kind of .

Mr. PICARSIC. It's really big. Yes.

Senator JOHNSON. Okay. Ms. Stokes, what would you say other than a romantic one? I kind of understand that one. What are some other ones? Because I want people watching this being alert when you see this, when somebody says, you know, like—go ahead.

Ms. STOKES. A big one is a tech support scam where you're on your device and you get a popup, and it says that there's a horrible problem with your device, and you have to call the number that they give. You react immediately because you're scared, and you call someone and it's the scammer. It goes from there, and it ends up involving accounts and getting money out of accounts through wires. It's very, very complicated, but to try to echo a little bit of what Nathan said, there are so many scams. Like, let's say, there are 80 scams, and each scam has red flags, like, say 10 red flags. That's 800 things to remember. It's exhausting for educators and for consumers who think that they're not going to be able to help themselves, right?

We take it up a level. It's sort of like the stop, drop, and roll for fire but this time, it's about recognizing three things that come

with most scams, and that's a contact out of the blue that yields heightened emotion and contains urgency and if we can train on that, we can also train how to take an active pause.

Senator JOHNSON. I would add a fourth. The one that if they ask you to call a number, or if they ask you to click on this site, would that also be——

Ms. STOKES. I'm trying to bring it up to a higher level there, because there's a million of those.

Senator JOHNSON. I mean, that you need to contact them, right? I mean, they need you to do something like open up this link, or.

Ms. STOKES. Yes. Click on a link, respond to a call, a phone number. We educate millions of people. I would say education is critical, but we're not educating our way out of this crisis. We need to be doing things to actually stop the scam from getting to the consumer to begin with.

Senator JOHNSON. Right. Ms. Koven?

Ms. BURNS KOVEN. Yes. I'll say from our perspective, Chainalysis just published research that found that impersonation scams have increased 1,400 percent in the last year. They're impersonating trusted individuals and entities, law enforcement, a known tech company, a cryptocurrency platform, or financial institution. Those are the hardest to weed out because those are—they are leveraging someone's trust in an entity that already exists.

I would absolutely echo Ms. Stokes' comments that the sense of urgency, especially. We're also finding increased payments from scammers in cryptocurrency to bulk SMS tools. They're coming for Americans on every platform that we rely on coming right to our phones and they're buying data lists with names, emails, phone numbers of Americans to target in the hundreds of thousands.

Senator JOHNSON. Okay. Thank you. Mr. Bagdoyan?

Mr. BAGDOYAN. Yes. Thank you, Senator Johnson. I think my fellow witnesses have covered most of the space here, but I would say investment scams that promise exorbitant returns with little or no risk, such as 1,000 percent. I get them by mail or text almost on a weekly basis. ″Send us $1,000, you'll have $1,000,000 by the end of the year.″

Well, that's great, but you know, it goes into the in the garbage bin. You have to be alert, if that's just too good to be true.

Senator JOHNSON. Okay. Well, thank you very much. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Warren.

Senator WARREN. Thank you, Mr. Chairman. I want to thank you and Ranking Member Gillibrand for holding this hearing. You know, falling victim to a scam is devastating for anyone, but it can be especially hard for seniors. When older Americans are taken advantage of, it's important for them to have someone to turn someone who will be on their side, someone who will help out, and that's where the Consumer Financial Protection Bureau comes in.

The CFPB is a financial cop on the beat for American consumers since 2011. It has saved over $21 billion for hardworking families, $21 billion, and that's not all it's done. The CFPB has a dedicated office to protect older Americans from financial fraud. It also has a consumer complaint database where people who've been ripped off can report scams and get their money back.

Mr. Bagdoyan, the Government Accountability Office, GAO, just conducted a review of federal scam prevention efforts. Can you explain how the CFPB protects Americans from scams, including seniors?

Mr. BAGDOYAN. Sure. As you know from our report, we identified CFPB as one of the three entities that are best positioned to lead the governmentwide strategy that we are advocating for. CFPB has the resident expertise. It has the legislative charge and mission, if you will. It has the experience since the early 2010's, as you noted, so, combined, those things are important.

We made five recommendations to CFPB to further its ability to counter scams in coordination, as we mentioned, as part of the governmentwide strategy to create the definition of scams, to gather better data, to analyze data and find out what the real risks are.

This is a very dynamic environment, but what it has been doing—I think it does all 11 categories of activities that we identified among the 13 agencies that were in our universe. It is well positioned to react through regulatory actions, through education, advocacy, and analytics. Again, it justifies them being well positioned to——

Senator WARREN. Yes. A lot of opportunities there in the way it's structured both to catch the bad guys and to be able to respond——

Mr. BAGDOYAN. That's right.

Senator WARREN [continuing]. and to be able to help people who've been cheated and get their money back for them. One of the points you make, though, is CFPB does not act alone, and that the three principal actors in this area are the CFPB, the FBI, and the FTC. I think I have that right?

Mr. BAGDOYAN. That's correct.

Senator WARREN. Three of them working together. I think one of your recommendations was that they should coordinate even more——

Mr. BAGDOYAN. Oh, absolutely.

Senator WARREN [continuing]. in their efforts. Is that right? Would you like to just say a word more about that?

Mr. BAGDOYAN. Yes, absolutely. That would be one of the key components of a governmentwide strategy. What we found was, of course, the 13 agencies that were working independently, coordinating on an ad hoc basis, but not systematically. That sort of fragmentation really undermines the effectiveness of anything any of these agencies do.

Senator WARREN. Not enhancing effectiveness, not more efficient when they fragment.

Mr. BAGDOYAN. That's right.

Senator WARREN. Based on what you've said here, you'd think that to protect seniors from scams that President Trump should leverage the CFPB. Unfortunately, that is not what he is doing. Instead, he is systematically dismantling the agency, cutting funds, cutting staff, and preventing the agency from doing its job.

Mr. Bagdoyan, let me just ask you, does cutting staff, cutting funds, issuing stop-work orders at the CFPB make seniors more safe about the same or less safe?

Mr. BAGDOYAN. Well, thank you for your question. I'm glad you asked it. It's very timely. As you may know, you submitted a re-

quest to us for follow-on work on staffing and organizational restructurings at the agencies. We may identify what kind of impact this would have on agencies' abilities to implement our recommendations, for example, and do a better job of protecting seniors and others against scams. Ranking Member Gillibrand is also a party to that request, and also, Senator Hassan, I believe, has joined recently. We staffed that review this morning.

Senator WARREN. Oh, good.

Mr. BAGDOYAN. We'll be starting that in several weeks. By spring, we should have a decent idea what our strategy to pursue that will entail. CFPB is one of the agencies that we will review for impacts any of these restructurings, including staff reductions, diversions, and other things. Thank you for your timely question.

Senator WARREN. Well, thank you very much. I appreciate the work you're doing. I want to say a very special thank you. Thank you to Senator Gillibrand and to Senator Hassan for joining in this effort. You know, if President Trump really cared about seniors, he would stop these illegal efforts to shut down the CFPB. CFPB is on the front lines trying to protect our seniors, and we need to offer its support so that it can do that important work.

Thanks very much. Appreciate it. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Warren. Mr. Picarsic, based on your research, would you say that the Chinese Communist Party is actively benefiting from the billions being stolen from American families?

Mr. PICARSIC. Yes. They disproportionately flow back into the Chinese banking system, so, yes.

The CHAIRMAN. All right. If we don't stop this, what's going to happen over the next five years? Are they going to—do you think they'll just continue to get bigger and bigger?

Mr. PICARSIC. Yes. We've seen exponential scaling over the past couple years that will continue. Worse, still, will be the fact that the cost of capital in the Chinese ecosystem will decrease and funds will flow into criminal enterprises, but also into the other nefarious efforts that the Chinese Communist Party pursues, including modernizing its military, modernizing its ecosystem for abusing other human rights.

The CHAIRMAN. It's a pretty good profit center for the Chinese.

Mr. PICARSIC. Absolutely.

The CHAIRMAN. Yes. Kathy, how much do you think it is now? You think it's almost $200 billion?

Ms. STOKES. Yes. That's based on the Federal Trade Commission's own analysis of underreporting.

The CHAIRMAN. Put that in perspective. We only have about a $28 trillion economy.

Ms. STOKES. I can tell you that if it was a Fortune company, it would be Fortune 17 in revenue.

The CHAIRMAN. It's hard to believe. What do you think is the single biggest failure in our current federal response that allows foreign criminals to keep targeting American seniors?

Ms. STOKES. Thank you, Senator, for asking that. I would say there are so many, but I would start with we need a national fraud strategy. We don't have that. We're seeing some good indications of having one, having some success in England and in Australia,

and they look to the United States and say, ″Okay, who's my counterpart?″

We have nobody. We need essentially a fraud czar in the administration coordinating efforts across the many agencies, but also coordinating with a private sector, law enforcement using data-driven means of being able to understand how these crimes individually tie together to get that organized crime connection to make the cases big enough to actually investigate, pursue, and prosecute.

The CHAIRMAN. Is there any federal agency that has a dedicated group of people doing this?

Ms. STOKES. I believe there are, yes.

The CHAIRMAN. Okay, but they're not coordinated.

Ms. STOKES. We could use some better coordination, yes.

The CHAIRMAN. Okay. Ms. Koven, when y'all track stolen funds from pig butchering and investment scams, where does the money typically flow, and how quickly does it move out of the reach of the individual and law enforcement?

Ms. BURNS KOVEN. Thank you for your question. The funds typically aggregate in consolidation wallets. One victim in Iowa's funds are commingled with a victim in Florida, with a victim from Illinois and we see these smaller payments aggregate in these larger consolidation clusters, which signal the centralized efforts of these scam conglomerates, and then they offboard into Chinese money laundering networks.

We see the yuan, which had special measures applied to it by the Federal Government, as well as other successors, guarantee services mostly Chinese language money laundering services. We do see a degree of centralized exchanges in DeFi services that do receive some of the funds.

While these movements are pretty rapid, we do have opportunities at these consolidation wallets that hold funds for longer periods of time. One of the challenges is that communication between private sector and public sector, connecting that victim in Illinois to that victim in Florida to see the bigger picture.

The beauty of blockchain intelligence is that you're able to unravel that entire picture without filing a single subpoena and working with private sector law enforcement has had stunning successes in seizing funds. Just this year, $15 billion seized from the Prince Group. We've had examples of hundreds of millions seized with the help of cryptocurrency exchanges and stablecoin issuers.

There's a lot of potential, but timing is on the line. Timing is at the essence. That's why we advocate for also a preventive strategy moving upstream so that scammers never interact with a human being.

The CHAIRMAN. When they get the money back, where's the money go? How much of it gets back to a victim?

Ms. BURNS KOVEN. That's a long legal process of you have to establish that you were a victim. Thankfully, the blockchain has a very clear trail of where a victim withdrew their funds in order to deposit it into a scam. I think there could be more clarity around that process to streamline it so that victims can be made whole.

The CHAIRMAN. How central are overseas networks particularly those linked to Communist China and Southeast Asia to the cryptocurrency scams targeting American seniors?

Ms. BURNS KOVEN. Yes. There are several data points from the cryptocurrency perspective pointing to China and Southeast Asia. The off ramps where these stolen funds are going are primarily offshore APAC-based services, Chinese money laundering networks where they have mules guarantee services. We're also seeing them reinvest their scam profits into additional AI tools, additional SMS scamming.

The CHAIRMAN. It's a business model.

Ms. BURNS KOVEN. Absolutely. It is a corporation. It is a well-oiled machine. We also see dips in cryptocurrency scam activity during Chinese public holidays and Chinese New Years, very much in line with China-based actors.

The CHAIRMAN. When people are working.

Ms. BURNS KOVEN. Absolutely.

The CHAIRMAN. Okay. Ranking Member Gillibrand.

Senator GILLIBRAND. Thank you. Mr. Bagdoyan, in a report, the GAO recommended that the FBI be the lead effort to develop a national strategy on scams. The legislation that Chairman Scott and I introduced, the National Strategy for Combating Scams Act, reflect GAO'S recommendation, and it would require FBI to lead the interagency effort.

However, while working on the report, you talked to 13 agencies that engage in efforts to combat scams, including the CFPB and the FTC. Conceivably, one of the other agencies could also lead the effort to develop the national strategy. Can you explain the GAO recommendation that the FBI lead the effort instead of the other agencies like the FTC?

Mr. BAGDOYAN. Sure. Thank you for your question, Ranking Member Gillibrand. The FBI, on balance, given all the factors that we reviewed, is best positioned to take the lead. They actually volunteered to do that while other agencies basically demurred either explicitly or implicitly. We took that into consideration.

We did make 16 recommendations to three agencies, as you know, but we thought that the FBI, has its scope, scale, its investigative capacity, its financial crime section — which is a key unit within the Bureau to tackle these types of crimes, including scams — its authorities and its global networks coordinating with other law enforcement. It's a multiplicity of factors that position them well to do this.

Senator GILLIBRAND. Thank you. Ms. Koven, in furtherance of Senator Scott's question about getting remuneration for the victims because of the blockchain, what tools would be useful in the Federal Government to have to be able to actually recoup some of that money? For example, do we need to augment the capabilities of FinCEN? Do we need to have a special directed unit to do cryptocurrency blockchain investigations for quick return of funding?

What recommendations do you have for us to specifically have more tools to use the benefits of the clarity and the transparency of the blockchain, but also to create better oversight and enforcement?

Ms. BURNS KOVEN. Thank you for your question. I can't speak to any specific agency, but I will say in my experience, there definitely needs to be more training and tools using blockchain ana-

lytics to be able to see the full spectrum of the crime, and so that we can holistically tackle the scam ecosystem, not just the scammed funds, but the services and infrastructure that are that are supporting and underlying these scams, from AI tech to data brokers.

We need to beat them at their own game. We can do that by incorporating AI-enabled fraud prevention strategies. Chainalysis' Alterya, for example, leverages AI to identify scam activity across platforms, payment system domains, social media accounts and blockchains. This enables financial institutions and law enforcement to identify more victims, build a bigger case, identify targets for disruption.

Frankly, this also allows this data to be integrated with financial institutions so that they can prevent scammers from even interacting with a human being before they even engage with the scam itself. In addition to recovering funds and restitution, prevention should absolutely be part of the strategy.

Senator GILLIBRAND. We frequently hear about the growing use of AI, including generative AI in scams that target older adults. However, the same technology that helps scammers may also be used to combat these scams, as you said. The Australian telecommunications firm, TPG, recently used AI chatbots to waste the time of scammers. You also discussed in your written testimony how Chainalysis has an AI tool that can help block scams.

Can you please discuss further how AI can be used in identifying and blocking scams? Do you foresee any new opportunities for tools to combat scams based on new developments of AI?

Ms. BURNS KOVEN. Absolutely. Thank you for that question. In our recent research, we found that scams leveraging AI are 4.5 times more profitable than scams that don't. We're rapidly approaching a future where virtually all scams will incorporate AI to some extent, which is pretty scary stuff when you think about the numbers they're pulling in today.

We do need to fight fire with fire. AI-enabled fraud prevention technologies like Chainalysis' Alterya, it leverages AI to identify scam activities across domain, social media accounts, and blockchains. This can enable financial institutions and blockchain companies to be able to integrate this into their platform so that they can identify mule accounts, victim accounts, and really have a holistic picture of the whole scam supply chain.

Furthermore, law enforcement also needs to have this prevention capability and this insight to be able to target their efforts against different components of the scam supply chain.

Senator GILLIBRAND. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you. Mr. Bagdoyan, the GAO said that the federal agencies aren't really coordinated. How does that impact somebody that's—you know, if they had better coordination, how would it save seniors money?

Mr. BAGDOYAN. Oh, that's a good question. There might be a way to cross reference approaches by a particular older American who goes to the FBI, because that makes sense to them, when the FTC might be better positioned to help them, or the CFPB for that matter, or some other agency.

There isn't a close-knitted approach to doing that, for example. I mean, that is a basic service that should be available. It isn't available. There are some agencies that accept consumer complaints, but they will refer the consumers to their own online educational materials, for example, rather than saying, ″Well, thank you for your call, but you should have gone to X.″ I don't think that's happening.

The CHAIRMAN. Mr. Picarsic, given your research on CCP, is it fair to say that the Communist China, the party, tolerates or turns a blind eye to these scam compounds because they want to weaken the United States?

Mr. PICARSIC. That's the most generous interpretation, that they turn a blind eye. I think more nefariously, they actively support and abet whenever they have a chance to.

The CHAIRMAN. How can you describe the level of coordination between these Chinese criminal networks and Communist China's broader geopolitical goals?

Mr. PICARSIC. They look to produce profits that can flow back into the Chinese ecosystem. They look to generate the capacity to project misinformation, and to sow dissent, and divide in the societies that they target. That may be the ones where they're operating from and maybe the ones that they're targeting.

We see from the layout, the geographic layout, the places that get populated with scam compounds tend to coincide with the places that dot the Belt and Road Initiative that have presence of Chinese international banking operations and all of these work together, perhaps not with smoking guns appearing at every turn, but with a whole host of loaded guns that can be pulled when they need to be.

I think the recent case that's been cited of the Prince Group is a telling example of a massive operation that was able to evade scrutiny in Cambodia for a long time. We recently indicted the leader. He was extradited not to the United States, not to our authorities, but to the Chinese.

He was able to be extradited to China because the Chinese government is active in courting Cambodian business and political elites. These channels all overlap, and when, and if they're needed to coordinate and work together, they do.

The CHAIRMAN. If Beijing wanted to shut this stuff down, could they do it?

Mr. PICARSIC. They absolutely could. For better or worse, they respond only to shows of strength and declarations of the capacity to control escalation dominance. For that reason, I think that American strategy needs to target the international presence of Chinese banks.

It's commendable that several pieces of legislation that the Committee's advanced cite IEEPA authorities, those authorities should be invoked and they should be used to target seizure of Chinese banking and Chinese banking leadership assets present in the United States.

The CHAIRMAN. Based on what you're saying, you would not suggest we ever buy things or do any business with China, is that——

Mr. PICARSIC. Absolutely. I think we have a consensus around strategic goods and the national security supply chains. Across the

board, American societies depend on Americans working together and American businesses thriving at all levels. If we allow even our most non-strategic assets to be fully offshore to an adversary, we're imposing on ourselves, for no reason, that opportunity cost.

It's not just the cost of that sector. It's the opportunity cost of that sector thriving somewhere else and not contributing directly to American society.

The CHAIRMAN. Kathy, can you talk about you—I know AARP's putting a lot of effort into this. Can you give a success story?

Ms. STOKES. Well, we probably talk to about 100,000 people every year through our helpline and we're not in a position—we're not law enforcement, we're not social workers, but we are able to talk to people in a sort of shame-free zone. We can't get their money back, but we can offer emotional support and we created a fraud support Zoom session, small group Zoom sessions, several years ago. Some of the people that have come through are here with me today.

What we do see in the success is that people begin to understand that it wasn't their fault, that they're not alone. They rebuild a sense of self. They build a sense of agency, and then they want to do something about it. We have victims telling their own narratives to law enforcement, to industry, to try to help people understand from that victim impact stance how nefarious these are.

The CHAIRMAN. Yes. Probably if somebody was a victim, it's probably better opportunity than somebody would listen to them also. Right?

Ms. STOKES. Well, we have a YouTube series called Fraud Wars that we just launched at the end of—well, actually, it was last summer. It's like these little 11 or 12 minute very highly produced videos, and it's the first-person narrative. They're very captivating.

The CHAIRMAN. Ms. Koven, based on your analysis, can you describe the lifecycle of a typical crypto-enabled scam targeting seniors from the first contact to a final launder in the funds? Give us an insight of how it happens. Let's say I'm the victim and you're trying to take advantage of me.

Ms. BURNS KOVEN. Thank you for the question. We don't often see the full lifecycle. Sometimes, we get information after the scam has already occurred. I can say that we are able to use our analysis to find when a victim makes recurring payments, and we've been able to do analysis on specific scam typologies, separating out pig butchering, versus blackmail, and extortion scams, from other scam typologies to understand which scams elicit recurring payments from a victim so we can see how effective they are in continuing to bleed out victims of their life savings versus ones that are shorter-term.

We are seeing a growing number of scam typologies, which I think is really interesting in the conversation of defining what a scam is because these scammers are relentless in capitalizing on new technologies, new flavors of the day. We're seeing different typologies leveraging working from home, for instance, which is a different on chain presence than maybe an impersonation scam, and we see the typical services recurringly used for laundering.

The blockchain shines a bright light on these services that continue to operate and process scammed funds. While the special

measures on huawan, for example, are very encouraging, as the largest, most prominent service that facilitated scams, there are others there are definitely successors waiting in the wings and know that scammers hedge their bets and are present on multiple different underground forums and guarantee youth platforms to continue their operations.

Anything that injects friction in these conversations, injects friction in their laundering, their trust in the different services, and imposes cost on all the key components of the supply chain are welcome and should be part of a national strategy.

The CHAIRMAN. Is China and Southeast Asia, are they a majority of the scammers?

Ms. BURNS KOVEN. I would say it's certainly a model that is highly effective. Not all scams originate from China or Southeast Asia, but it is setting the model for what we fear other jurisdictions, other scammers, other organizations could adopt.

The CHAIRMAN. Is information sharing helpful?

Ms. BURNS KOVEN. Absolutely. I appreciate this Committee's attention on ways we can streamline information sharing. There are so many different entities where a victim can report their scam, but also many don't.

The blockchain is effective in highlighting payments of victims that may have not reported. We should use that intelligence to drive our mission to be able to instead of one-off investigations, we grow the amount of funds that are feasible and reduce friction amongst these agencies.

Overall, we have to increase a public-private sector information-sharing too. Because a private sector entity, say a financial institution, that files a suspicious activity report about a scam on their platform, the bank next door will never get wind of what was in that scam.

They're encountering the same adversaries. Their customers are being targeted by the same adversaries, yet, they cannot share information. Private sector is best positioned to prevent future scam victims. We need that quick information-sharing, and the whole-of-government, as well as whole-society approach.

The CHAIRMAN. Ranking Member Gillibrand.

Senator GILLIBRAND. Ms. Stokes, can you talk a little bit about the proposal to have local elder justice task forces? What effect do you believe these task forces could have on efforts to combat scams?

Ms. STOKES. Thank you, Senator, for the question. I think they're critical. The elder justice task force model allows for coordination among local, state, federal law enforcement, prosecutors, also agencies of adult protective services, things like that. It helps the ability for data to be gathered and assessed to be able to start to see patterns. That's that pattern that we're missing right now because we're not looking at it through an organized crime lens.

I have many examples from the San Diego Elder Justice Task Force that they've done some amazing things, very much because they are an elder justice task force, and they are looking at data and being able to understand tying things together and going after big cases. I think it's really important.

Senator GILLIBRAND. What are the biggest barriers for seniors to come forward to report when a scam has happened? What are their barriers for seeking help, and what are the best ways to help them rebuild their lives after a scam? You mentioned the relationships and the communities you're creating throughout AARP. I think that's really terrific.

I do think we should, for example, the person that you talked about who lost all that tax money, I could get that tax money back for her. I think we should have lawyers who can make the case that through artifice and fraud, they do not owe taxes. At least she'd get that $200,000 back, so she'd have part of her savings. Maybe even having legal services available for scam victims to get some kind of recuperation.

Ms. STOKES. Yes. Thank you, Senator. She's certainly not alone. We have many victims that come through this process, and because the money was taken from a tax deferred retirement plan, they end up owing the taxes because the IRS looks at it as income.

Senator GILLIBRAND. We can probably change that law.

Ms. STOKES. We would like to see that changed. There's a bill out there now, as a matter of fact.

Senator GILLIBRAND. Yes. Well, I'll work on that, and I'll also work on your task force bill.

Ms. STOKES. Thank you very much. In terms of the barriers for victims, one of the barriers is sort of internal. They're so ashamed, so embarrassed, they think it only happens to them. That comes from a society that has tended to blame victims for the crime that has happened and we've done that for years, and we've allowed ourselves to believe that it's only old people who aren't tech savvy, who may have cognitive issues and so it's sort of a them problem.

Now we're starting to understand that it's an all-of-us problem because everybody is being targeted. You don't have to have cognitive decline because of the sophistication of the playbook that the criminals use. We're seeing some change there, and then the other is there's just too many calls to action. You know, you could report it to the FBI, and FTC, and the Social Security Administration, and everything else. We need a single door that consumers can go to, victims can go to, not only to be able to report, but to report it into a law enforcement system where the data are going to be connected to other reports so that we can begin that be better at the organized crime connections there.

Also importantly, so many people that report they never hear anything, especially if they report something online. They're expect—they're hoping for a call. We need a system where people are treated with dignity and respect, and that there is some outreach that lets them know what's going on, even if nothing's going on, to make them feel less like it was their fault.

Senator GILLIBRAND. Mr. Picarsic, can you talk a little bit about what type of international joint ventures we should be trying to have with our allies? I'm certain it's not just American seniors who are being targeted. I'm sure it's true across the whole globe but I can imagine if we had international coordination with the UK, or some of our EU allies, or Asian or Middle Eastern allies, we could crack some of these criminal networks a lot quicker.

Do you have any recommendations for us with regard to coordination of investigations?

Mr. PICARSIC. Thank you very much for the compelling question. I think it tracks with the way that we've been able to share information, increase early warning, and coordinate action in similar realms of criminal activity, including cyber threats. The way that across our international relationships, we've been able to build multilateral fora and support law enforcement.

I think it starts with information-sharing and we have existing fora from cyber, and counterfeit, drug, and counter smuggling activities that can be activated the same way. I think it's a compelling priority, and one that we have infrastructure to pipe the right information through.

Senator GILLIBRAND. Then last, can you just explain why human trafficking is often associated with these types of scams?

Mr. PICARSIC. Yes. Chairman Scott has mentioned just how profitable and good a business these operations are. Part of their fundamental orientation is that they're leveraging trafficked humans so that they don't even have a payroll. They tend to be populated, again, in these territories where there may be lax oversight and are hotspots for human trafficking.

Then there's overlap with the actual people leading compounds and moving money with human trafficking. They're able to take forced labor and employ them in compounds, and also, to shield themselves from any scrutiny from local as well as Chinese authorities.

Senator GILLIBRAND. Terrible. Thank you, Mr. Chairman. Yes, I'm done.

The CHAIRMAN. Senator Moody.

Senator MOODY. Thank you, Chairman Scott, and Ranking Member Gillibrand. Such an important topic to all seniors in America, especially my home State of Florida. We are a premier destination state for seniors moving there in retirement. We often call ourselves not just the Sunshine State, but the Silver State and as technology has advanced so rapidly the tools that criminals will use to scam our seniors has multiplied.

I realized this very quickly in my background. I served as a federal prosecutor, as attorney general. I understood very quickly that the federal standards sometimes for investigation and prosecution in terms of monetary loss, the bar to reach that becomes so high that we're often, if we're not aggregating smaller amounts to show these larger losses in the aggregate, sometimes those fall through the cracks.

It's oftentimes those lower amounts and I say lower only because it's relative to the sometimes hundreds of millions of dollars we might see in one scam compared to if you aggregate, let's say numerous seniors get taken advantage of. It could be their life savings and even when you aggregate that, it could be a lot, but if you don't know that they're related, it might seem not to reach the federal levels of investigation.

What I found very quickly, a huge gap in enforcement investigations, prosecutions, bringing criminals to justice, is the inability of states to match sometimes the manpower and coordination at the federal level, the capabilities to go after these people.

As Florida's AG, one of the first things I did was put together a cyber fraud enforcement team to start looking at these things to cooperate with the federal officials, but start bringing in experts into the investigation side and the prosecution side because both are so important, and it does require a specified expertise.

We saw results immediately, not only in going after those that might have fallen through the cracks, those specific cases but also recovering funds, freezing assets, even cryptocurrency.

I think this is so important, and I'm so glad, Chairman Scott, thanks to have these hearings because oftentimes it's foreign nationals that are using this advancing technology to victimize Americans, Floridians, and they're never brought to justice because they're overseas and we become put in a position where we're just trying to prevent, educate and that's so important, but we have to have the teeth to come back and hold these people accountable.

I have totally foregone anything I planned to ask, but I would just like to get from you. We did this as kind of it was an initiative in Florida. It is now bearing fruit. It's still in existence. They're freezing funds. They're going after people.

In fact, just recently that that same cyber fraud enforcement unit that I started seized $1.5 million connected to an internet-based investment scheme that was perpetuated by a Chinese national. I'm so proud of what we were able to accomplish there.

I would like to open this up, with the chairman's permission. If any of you could comment on how I often am very reluctant as an idea to just throw more money at a problem but if the goal is to get more states to start their own cyber fraud enforcement units that can coordinate with the feds, but also begin to bring their own expertise to bear and start these units to help their state, their county and city.

If you have a state cyber fraud enforcement unit that can lay over expertise in rural counties and cities that might not have that. It was so effective in Florida and I'm wondering if any of you believe or have recommendations on how we, as a Federal Government, might encourage more state cyber fraud enforcement groups.

I saw how effective that was at filling the gap in Florida. Anyone want to chime in on this? Do you have any recommendations, for us as Senators, on how we can make that happen?

Ms. BURNS KOVEN. Thank you for your questions, Senator. I'm delighted to hear about some of the successes you've had. That's fantastic. Because you've laid out some vast challenges, right, which is information-sharing, connecting a victim in Florida to the same scam of somebody out of state or even out of the country.

Blockchain analytics has been the common language and visibility for so many successes for scam funds recovery, putting crossing that bridge between private and public sector so that a private sector can prevent additional scam victims from falling prey but I think more so we need to make sure state, local, and federal law enforcement, and regulators have the tools and training they need to be able to understand crypto cases.

We hear often that victims are turned away because they don't know how to investigate crypto cases, or that the case is too small to meet a threshold, when in reality, that one scam victim sends

funds to a multimillion-dollar scam conglomerate where there's a ripe opportunity for intervention and asset seizure.

In addition to recovering funds and restitution, we also have to bring the fight to the scammers. We need to focus on prevention, making sure those scammers never interact with a human and we can do that through AI, which Chainalysis' Alterya, for example, leverages AI-enabled fraud prevention to be able to collect scam identifiers from across online infrastructure, from platforms, from payment systems, from domains, to social media.

Being able to connect victims but also identify scam infrastructure so that financial institutions and crypto businesses don't even permit that activity on their platform. It also is enabling for law enforcement to better target for disruption, what are the key nodes that are underlying this scam ecosystem.

Senator MOODY. Thank you. I have to say, my staff told me you would know a lot about that. I appreciate it. Thank you for making them look really good. I wish I could show you. It says right here, ″Ask Ms. Burns Koven.″ Thank you very much and to all of you for being here today. We really appreciate it.

The CHAIRMAN. Thank you, Senator Moody. I want to thank everybody for coming today, being and participating. I also want to remind seniors and families watching that the Senate Aging Committee operates a fraud hotline for anyone who believes they may have been targeted or victimized. The number is 1–855–303–9470. Nice, easy number to memorize.

If any seniors or any Senators have additional questions for the witnesses or statements to be added, the hearing record will be open until next Wednesday at 5:00 p.m. Thanks, everybody.

[Whereupon, at 4:48 p.m., the hearing was adjourned.]

APPENDIX

Prepared Witness Statements

TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

Senate Special Committee on Aging

Made in China, Paid by Seniors: Stopping the Surge of International Scams

NATHAN PICARSIC

Senior Fellow
Foundation for Defense of Democracies

Washington, DC
January 14, 2026

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

I would like to thank Chairman Scott, Ranking Member Gillibrand, and committee members for the opportunity to join today's hearing and offer testimony alongside my esteemed co-witnesses. I would also like to thank the committee members and staff for convening this hearing and dedicating effort to crafting thoughtful legislation to support American elders and families impacted by elder scams.

According to FBI analysis, the elder scam marketplace already accounts for billions of U.S. dollars in harm annually. China and Chinese-linked operations play an outsize role in executing and supporting these international scams. That constitutes a direct threat to America's elderly population and to American society.

In this testimony, I hope to convey three points about the threat: The strategic implications of international scam operations and their relevance to great power competition between the United States and China; the complicit nature of the Chinese government in the proliferation of scams that target elderly populations in the United States; and the need for legislation and federal government leadership to empower coordination between federal authorities, law enforcement, and the financial ecosystem that can disrupt and deter China-linked scams against Americans.

Elder Scams and Strategic Competition

The strength of the United States, both domestically and as it stacks up against international competition, is a function of the whole of American society. America is at its greatest when confident in its domestic cohesion. That cohesion has historically stemmed from a social contract that provides opportunity for life, liberty, and the pursuit of happiness; it requires trust backed by the rule of law, transparency, and justice. Those features set America apart. They make everything from our capital markets to our universities to our farms the envy of the world. But American institutions and the American experiment writ large did not emerge without struggle, and they will not be sustained without vigilance.

America should lead. Leading requires, on the one hand, openness to the world and, on the other, concomitant investment in protecting against the risks that openness invites. Mastering that balance is a key to American greatness. Nothing better reflects the importance of getting that balance right — and signals to our competitors our sincerity and resolve — than how we protect our most vulnerable.

Social cohesion is a pivotal battleground in today's international contest. Defending against external attacks targeting our vulnerable, including our elderly, is a fundamental, if nontraditional, requirement for succeeding in long-term, peacetime competition.[1]

[1] Emily de La Bruyère and Nathan Picarsic, "Wanted: A Strategy for Long-term Peacetime Competition with China," *Foundation for Defense of Democracies*, June 1, 2020. (https://www.fdd.org/analysis/2020/06/01/strategy-for-peacetime-with-china)

China understands this. And China deliberately positions itself to foment fissures within American society and to tease at American vulnerabilities.[2] It is not uncommon to hear about this Chinese tack in the context of malign foreign influence in narrative and media, foreign investment that carries national security risk, or efforts to capture elites across American society. The same underlying, competitive ambitions that propel those hydra heads of China's global influence campaign also propel the transnational criminal forces that execute, guide, and redeem proceeds from elder scams in the United States. Chinese criminal actors have been prosecuted for roles in leading elder scams in the United States. But recognition of the full scope of this threat lags. So, too, does marshaling a right-sized response.

State-Backed Scamming

Scams targeting elderly Americans know no political or socio-economic boundaries. If you have an aging parent, grandparent, or neighbor, you've certainly heard the harrowing tales and very likely also know the implications, personally, of these attacks. Elder scams generate stress and devastation for targets, victims, and their families all across the United States.

These scams also know no borders. Scam operations are big business. And they are international. China plays an outsize role in the expansion, proliferation, and nefarious success of these scams. China plays this role both in scams that originate in China itself and outside, in hotspots across Southeast Asia, where scam operations exist and scam compounds operate under Chinese leadership. Chinese-linked scam operations feed into a broader network of transnational criminal efforts. Those efforts are permitted and, at times, abetted by the Chinese state and its ruling Communist Party.

China's broader transnational criminal enterprise benefits from a permissive state apparatus in Beijing. The leaders of the Chinese Communist Party would much rather see criminal acts perpetrated against foreign targets than against China's own aging population. Accordingly, the Chinese government has allowed China's cottage industry of scam operations, including those that target elder victims, to exist — and to refine tactics, techniques, procedures, and international positioning that enable professional and adaptive performance.

China's scam networks are best-in-class, just as China's hackers have matured to pose persistent threats to critical global cyber networks. Unfortunately, global — and American — vigilance has not kept pace. And China has several fundamental advantages that make catching up in this hider-finder game a daunting task for relevant American authorities.

First, China's transnational criminal networks benefit from advanced technology — and the Chinese state's support for developing, fielding, and scaling that technology. Beijing pursues a "network great power" strategy.[3] The strategy is built on a backbone of communications network, including telecommunications network, capabilities that are directly transferable to transnational

[2] RADM (Ret.) Mark Montgomery and Annie Fixler, "China has a cyberspace campaign plan. Does Washington?" *Washington Examiner*, December 5, 2022. (https://www.washingtonexaminer.com/news/2871713/china-has-a-cyberspace-campaign-plan-does-washington)
[3] Emily de La Bruyère, "The Network Great-Power Strategy," *Asia Policy*, APRIL 2021, pages 5-16. (https://www.jstor.org/stable/27023967)

criminal operations and the tactics of common elder scams. For instance, Chinese industrial and technological capacity in networking equipment, cloud computing, artificial intelligence, and big data all help Chinese transnational criminal organizations generate, share, refine, and distribute English-language scripts for social engineering calls and chats that feed elder scams. Moreover, China's telecommunications champions have internationalized, along with Beijing's so-called "Belt and Road." This provides regional bastions from which Chinese criminal organizations can operate — and that the Chinese state can use for an added buffer of plausible deniability.

Second, China's banking sector has followed the same "Go Out" playbook as China's corporate sector. This has laid the financial foundation for Chinese scam networks to internationalize. China's rise as a global banking power allows China-linked criminal networks to transfer money across borders, obfuscate the flow of funds, and evade regulatory authorities. Chinese criminal networks often use bank outposts in Hong Kong to transfer ill-gotten gains and to obfuscate their ultimate destinations. As long as funds are flowing over Chinese bank channels, international — including U.S. — authorities are hard-pressed to guarantee compliance with basic anti-money laundering requirements, let alone keep pace with emerging threats like those presented by cryptocurrency.

The net impact of China's positioning is a new, global, and highly efficacious phenomenon of state-backed scamming. This phenomenon will continue to benefit from scale, technology, and a complicit banking ecosystem in China. As China increases its investments in advanced networking and communications and financial technologies, including crypto, China's criminal networks will benefit. They will become more adept at executing, and profiting, from elder scams. America's seniors will suffer the consequences.

Commendable work by the U.S. Department of Justice has documented how China's capabilities come together today to create a large-scale threat and commensurate impact.[4] Elder scams executed by Chinese-linked networks prey on a variety of populations but prioritize those known to be vulnerable targets — namely, individuals who are retired, have ample savings, and lack digital fluency. How do scam networks identify those targets? Through data brokers trafficking lists from previous hacks, including insurance hacks. And those hacks, in turn, are often the work of Chinese state-backed hackers.

"Pig butchering" (杀猪盘) has emerged as a term to describe certain cyber-enabled scams that frequently target elderly victims. That term traces back to Chinese, underscoring the foundational role of Chinese entities in shaping the tactics and networks that dominate the international scam marketplace.[5] "Pig butchering" scams originated in China. But today, they have been scaled in the United States, in many cases by Chinese operations, and target American citizens.

---

[4] U.S. Department of Justice, "Annual Report to Congress on Department of Justice Activities to Combat Elder Fraud and Abuse," October 2025. (https://www.justice.gov/elderjustice/media/1416301/dl?inline)

[5] The term was even included among a set of "top 10 new terms in Chinese media in 2019" and reportedly was first coined by Chinese online commenters: Ying Ni, "2019年度中国媒体十大新词出炉 夜经济、极限施压等入列 [The top 10 new terms in Chinese media in 2019 have been released, including 'night economy' and 'maximum pressure']," *China News* (China). (https://www.chinanews.com.cn/gn/2019/12-16/9034981.shtml)

For example, in May 2024, the U.S. Attorney's Office for the Eastern District of Texas brought charges against a Chinese national who allegedly attempted to commit wire fraud and money laundering crimes to move "millions of dollars." He had allegedly acquired those funds by convincing unwitting victims that they were investing in legitimate business opportunities via cryptocurrency.[6] That is just one case. In July 2024, the U.S. Attorney's Office in the Southern District of California brought charges against five Chinese nationals accused of "a massive, complex fraud and money laundering scheme." That case featured $27 million in funds alleged to have been acquired by fraud, with more than 2,000 American seniors among the victims of the indicted network.[7]

Dozens of additional cases of a similar scope have been brought to light over the past few years. But those cases risk being the tip of the iceberg. The true scale of Chinese-linked attacks is unknown; it is safe to assume that some multiple of the number of cases that have been discovered and prosecuted has actually played out — and that the pace of growth in Chinese-tied elder scams, whether measured in victims or value, will continue to accelerate in the years ahead.

Compounding the threat posed by Chinese-tied tactics and perpetrators is the power of the Chinese financial system in propelling them. Take, for instance, one "business email confidence" case in which the Department of Justice sought to recover funds that had been deployed through U.S.-based "mules." That case saw upwards of 5 million U.S. dollars fraudulently attempted to be routed out of the United States. In that case, the destinations for transfer of ill-gotten funds were allegedly Bank of China, Standard Chartered in Hong Kong, and Singaporean accounts.[8] And the problem isn't just that this internationalized Chinese banking system exists as a channel for funds. Worryingly, this channel makes it nearly impossible to reclaim stolen funds. Victims of elder crime often have little recourse after funds have been offshored and may see their entire savings drained. Moreover, those funds, in turn, become fuel for additional criminal activity. Technological advances across telecommunications networking and cryptocurrency will add additional fuel to this fire.

The systemic nature of China's scamming enterprise amounts to great power stakes. The U.S. — government, technology companies, and banks — cannot afford to stand by as Chinese-linked criminal networks deplete American social trust and bank accounts.

Defending American Elders

A whack-a-mole response will not solve the challenge at hand. State-backed, international scam networks have the resources and flexibility to outfox both their targets and the law enforcement authorities that are invariably playing catch-up once alerted to a case. To offset this imbalance, the United States needs to erect protections and sensing — akin to the use of anti-virus software — that provide early warning. The U.S. government needs to increase awareness of these risks and

[6] U.S. Attorney's Office, Eastern District of Texas, Press Release, "Chinese national charged in "pig butchering" scheme," May 21, 2024. (https://www.justice.gov/usao-edtx/pr/chinese-national-charged-pig-butchering-scheme)
[7] U.S. Attorney's Office, Southern District of California, Press Release, "Five Chinese Nationals Indicted for Scamming Seniors Out of More Than $27 Million," July 31, 2024. (https://www.justice.gov/usao-sdca/pr/five-chinese-nationals-indicted-scamming-seniors-out-more-27-million)
[8] See: United States v. Approximately $143,586.44 Seized From JPMorgan Chase, No. 1:24-cv-11467, June 5, 2024. (https://www.justice.gov/usao-ma/media/1354406/dl)

the common tactics leveraged by scammers to inoculate our most vulnerable and the institutions that support them. And the U.S. government must enforce aggressively against perpetrators to send a deterrent signal.

Legislation can help. In particular, the National Strategies for Combating Scams Act offers an orienting call for strategy. Its requirement for the rapid development of a national strategy aligns with the urgency of the risk. That bill's mandate to drive coordination across over a dozen relevant federal agencies will spur necessary interagency collaboration and information sharing. Similarly, the Scam Compound Accountability and Mobilization Act addresses the sprawling, global layout of scam networks that operate across Southeast Asia with backing from China-linked actors and that benefit from opportunities to launder proceeds through China's banking system. The act's tasking to the secretary of state will compel additional coordination across the interagency and enable targeting of Chinese equities through the proposed Enabling Country List mechanism. Those efforts can go a long way toward activating federal resources and coordination. That is a necessary first step to empowering law enforcement and local actors who stand on the front lines of supporting elder Americans and their families as they confront a tidal wave of China-linked scammers. Additional effort will be necessary to properly resource and provide information to those subnational and non-federal authorities.

At the same time, the great power stakes of the threat to America's elderly population underscore that, ultimately, protective measures need to deliver a deterrent effect in the adversary's system. In order to orient toward that objective, U.S. federal authorities across the interagency should prepare for and signal to Chinese counterparts the political will and practical capacity to effectively target the core nodes of the Chinese banking system that aid and abet crimes against American elders. Those nodes of the Chinese banking system are the same ones that fund China's military-civil fusion ecosystem and that move money to support coordination between Chinese chemical companies and international drug cartels. Imposing costs on those pillars of China's system would not just be good defense of America's elders, but rather it would be good strategy. Signaling resolve in this direction could be conveyed by documenting assets of high-risk Chinese financial institutions and their leaders that may be held in the United States and, as such, could be subject to seizure under authorities that could be triggered by the International Emergency Economic Powers Act (IEEPA).

Thank you for the opportunity to contribute to today's hearing and for the important work of the committee on these timely issues.

My name is Kathy Stokes, and I am Senior Director of Fraud Prevention Programs for the AARP Fraud Watch Network. I am honored to be here to testify on behalf of AARP, which advocates on behalf of 125 million Americans age 50 and older and their families. I would like to thank you and the members of the Senate Special Committee on Aging for holding this important hearing, "Made in China, Paid by Seniors: Stopping the Surge of International Scams." AARP has long worked to educate consumers, support fraud victims, and improve fraud detection and prevention across industries, and we look forward to working with you towards policy solutions to prevent fraud and protect consumers.

AARP Fraud Prevention Work

The Fraud Watch Network is AARP's program deeply vested in helping our nation's older adults understand the very real threat to their financial security that fraud represents.

We engage in communities around the country through all our state offices and their trained volunteer fraud fighters spreading the message of fraud prevention. We share robust information online at aarp.org/fraudwatchnetwork; we cover the issue in *AARP the Magazine* and the *AARP Bulletin* – which reach tens of millions of readers with each edition; we offer a biweekly email or text 'watchdog alert' newsletter and we produce an award-winning podcast, AARP's The Perfect Scam – in the true crime genre but focused on the impact of this type of crime on victims and their families. We also offer a variety of virtual educational events, from member teletown halls to webinars and Facebook live events.

In addition, AARP is unique in its focus on supporting victims of fraud and their families. Our Fraud Watch Network Helpline receives around 500 calls a day. These calls can be from people who simply want to report a scam they've encountered but didn't engage with, to people who aren't sure whether that Publishers Clearing House letter claiming they've won $1 million and a Mercedes is legitimate (it's not), and too often, from victims and their family members in the aftermath of the crime. We also offer an online victim support group program, through which trained facilitators run small group sessions to begin to address the emotional impact of fraud victimization—helping older Americans rebuild their lives.

On the prevention front, we know that education is critical, but we cannot educate our way out of the fraud crisis. AARP is at the forefront of seeking systemic change. For one, AARP has been leading an effort to reframe the narrative on fraud victimization. Our society tends to treat fraud victims differently than other crime victims. We often blame them with the language we use: they've been tricked, or duped, or fooled, rather than stating that a criminal has stolen from them. We tend to believe that there's nothing law enforcement can do because the criminals are abroad. Our narrative change movement is rooted in research that shows how our tendency to blame fraud victims has served to deprioritize fraud as a crime. From the start of our narrative change campaign with the FINRA Investor Education Foundation in 2021, we have continued the focus and we are seeing real movement – among consumers, in the media, across industries and among policymakers, toward an understanding that fraud is a crime and is not the victim's fault.

Additionally, AARP is proud to be among the founders of the new nonprofit National Elder Fraud Coordination Center (or NEFCC), which formally launched last April. NEFCC has not

only aggregated intelligence related to elder fraud from its members and provided packages to law enforcement, which was its original intent, but NEFCC has also taken existing criminal investigations and expanded them with fraud intelligence from its private sector members.

In one example, a federal investigation on a massive – but stalled – tech support scam case was reignited when NEFCC was able to transform scattered leads into a coordinated, multiorganization push. NEFCC's rapid analysis of the original case materials revealed a network of 24 U.S.-based shell companies receiving fraudulent victim funds tied to the broader criminal ecosystem. NEFCC launched a nationwide intelligence collection request to major banks, fintech providers, and digital asset platforms, which directly enriched the federal criminal investigation and filled prior intelligence gaps. The renewed collaboration, driven by NEFCC's orchestration, established momentum, validated investigative linkages, and positioned the federal law enforcement agency for the next phase of action against the domestic nodes supporting an international elder fraud operation.

The Fraud Crisis

The growth in fraud crimes over the past five years has been meteoric. For example, published data from the Federal Trade Commission (FTC) shows a reported $12.8 billion stolen through fraud against Americans in 2024. But this number doesn't begin to tell the true story. In a 2025 report the FTC submitted to Congress, the agency acknowledged the significant problem of under-reporting. Using its own estimates of under-reporting, the agency extrapolated that money stolen from fraud in 2024 was not the reported $12.8 billion, but more like $196 billion. And the agency pegged fraud losses among older adults at $81.5 billion.

Fraud criminals know no demographic bounds. They seek to steal money and sensitive information from targets regardless of age, educational attainment, or socioeconomic status. But when they victimize our nation's older adults, the financial impact is too often profound and life-altering. This stands to reason, as older adults are more likely to have accumulated a lifetime of savings and are more likely to have housing wealth. And, too often, the criminals steal everything. The victims are emotionally and financially ruined, often their families are torn apart, and many victims who were financially prepared for a secure retirement are instead left to rely on already strained local, state and federal safety nets.

The Criminals Behind Fraud

The driver of fraud's expansion since 2019 has been the growth of transnational criminal organizations behind much of the fraud we see today. Importantly, the funds they amass by stealing hundreds of billions of dollars from our nation's citizens through fraud represent a national security threat.

For example, we know that the Jalisco New Generation Cartel in Mexico is a major contributor to fentanyl and meth crossing our southern border. They are now known also to run timeshare resale scams targeting timeshare owners in the United States, which helps fund their illicit activities. Last summer, FinCEN put out an alert on this alarming new trend together with OFAC

and the FBI. We also know that illicit funds pulled in through ransomware and other attacks by the North Korea-backed Lazarus Group support the country's missile and nuclear programs.

In a highly sophisticated financial grooming scam with its origins in Southeast Asia, Chinese organized crime rings are stealing hundreds of millions of dollars from American targets. The *Economist* reported the experience of an individual who, through human trafficking, was enslaved to serve as a front-line scammer. He recalled the morning ritual where they all chanted things like "Death to the American Economy." This victim is but one of potentially hundreds of thousands of people who are victims of human trafficking that fuels this crime.

Why Scams Succeed

The days of snake oil salesmen and lone grifters have given way to transnational organized crime rings with corporate offices, employees (often enslaved prisoners forced by physical threat to be frontline scammers), lead lists, personally identifiable information (PII) from data hacks and breaches, scripts, and a playbook of how to turn a fraud target into a fraud victim. These criminal enterprises leverage a vast array of tools to commit their crimes, including all methods of communication and forms of payment, complex impersonation schemes, anonymous shell companies, and human trafficking.

But sophistication and scale alone aren't the reasons they succeed. The reason scams are successful is largely because of how the human brain functions. AARP's own research beginning decades ago unveiled what criminal scammers refer to as getting their targets "under the ether." They have known since the beginning of time that to trigger a heightened emotional state is to bypass logical thinking – it is how our brains work.

What criminals call getting the target "under the ether," academics refer to as an "amygdala hijack." The amygdala is the part of our brain that processes emotions. When the amygdala is hijacked, the part of our brain responsible for logic – the prefrontal cortex, is bypassed. It's important to recognize that victims don't become victims because of their age, educational level or cognitive impairment. They became victims because of how our brains have functioned for 300,000 years.

This message is critical as we seek to marshal a meaningful response to the fraud crisis. Until we all understand that fraud victims are crime victims and that they aren't responsible for becoming victims, we will fail to address this crime for the scourge it is.

Concerning Fraud Trends

The tactics of fraud criminals range from old school (stealing your mail) to high tech (hacks of banks, retail chains, and other companies that stockpile consumer data). They might pretend to be from the government, utility companies, banks, or big tech firms in order to steal sensitive personal information, or they send phishing emails with links that can infect devices with data-harvesting malware. Sensitive information is bought and sold among criminals on the dark web and via apps, which other criminals then use to better target their victims.

Methods of attack by these criminals span across communication channels: phone calls, emails, text messages, social media, online ads, and other pop-up messages, fraudulent apps, mail, and at times, in person. In other words, there is no form of communication that fraud criminals have not made dangerous.

Of the hundreds of fraud types in play, three are of particular concern: the tech support scam, the bank impostor scam, and financial grooming.

Tech Support Scams

A tech support scam may originate with a call from someone claiming to be with Microsoft or Windows tech support, or via a pop-up window on your device screen. The target is warned that a virus has been detected, and to protect their data, they must go to a web address or call a provided phone number. Inevitably, the "tech support" person convinces the target to allow them to remotely access their device, leading often to even more complexity to the scam and massive financial losses.

Helen, from Southern California, told AARP's Fraud Watch Helpline that she received a pop-up message on her computer screen along with a loud voice warning: "Do not turn off your computer!" Helen was instructed to call the phone number on her screen, and she soon found herself talking to someone who claimed to be a tech support staffer from Microsoft. The fake tech support staffer told her that her computer was under attack and convinced her to download software that gave him access to her computer and its data.

Helen didn't realize that the "helpful" technician was part of a fraud ring, and that the pop-up on her computer was a fake. He offered to put her through to the security department, where someone posing as a bank official told her that hackers already were stealing from her account, and she needed to quickly move her funds to a new, safe account. Helen followed his instructions, withdrawing cash, buying gift cards, and sending wire transfers and cashier's checks to addresses in other cities. Most of her retirement nest egg was stolen before a bank fraud investigator intervened, convincing her to speak to her family about what was happening.

Bank Impostor Scams

In this growing scam, a target receives a text message from what appears to be their bank, asking them if a certain transaction made on their account is legitimate, typically requesting a Yes or No response. The target sees a transaction they didn't make and responds No.

A phone call immediately follows, ostensibly from their bank. The caller explains that they are a bank fraud investigator and that their accounts are being actively hacked. The fake bank investigator then helps the target transfer their assets to keep them safe. The ending is always the same; it wasn't the person's actual bank and the victim's assets have been stolen with little chance of recovery.

Magis, who reached out to AARP's Fraud Watch Network Helpline, experienced this scheme. She was made to believe that her bank's fraud investigators were seeking to help her address

fraud in her accounts. They told her that her stolen identity was being used by foreign cybercriminals who used it to buy child sexual exploitation materials, murder people, and sell body parts. The impact grew to affect her retirement account, and more than $1 million was stolen throughout the scam. Magis has suffered significant stress and faces the possibility of being forced to sell her home and face homelessness.

Financial Grooming

Romance scams are sadly common, where a victim is manipulated over time to believe they are in a deep love affair with someone they've met online, only to be crushed when they learn it was all a lie and their savings had been wiped out as well.

A more recent form of this scam typically begins with what seems like an errant text message such as, "Hey Bob, are we still on for dinner at 7?" The recipient kindly responds to tell the sender they have the wrong person. And that is all it takes to build out a conversation, that turns into a friendship that becomes a trusted relationship, that leads to a devastating investment fraud that destroys victims emotionally and financially.

In this particular scam, there are victims on both ends of the crime. Southeast Asian organized crime groups lure frontline scammers with fake job offers. Once they arrive, the criminals take their passports and force them to phish for potential scam victims for endless hours a day under threat of violence and even death. This crime is dubbed by the criminals who came up with it, Pig Butchering – where they fatten the victim before slaughter. The term is so loaded with victim blaming that many in this space refer to it instead as financial grooming. Through an in-depth investigative report from *The Economist* published in February, readers learned that a stated goal of this crime is to "cripple the US economy."

Their targets are groomed over weeks or months and at some point, the scammer explains that they have such a great life with cars and homes and jewelry because of their investments in cryptocurrency – and they can show the target how to trade. The scammer convinces the target to access an online or app-based crypto exchange and encourages small investments at first. The returns entice the target to invest larger amounts, and the returns continue to grow. When the victim decides it's time to cash out, they are told they first have to pay thousands in taxes. The victim may even cash out other accounts to pay the taxes, only to find that the entire ordeal was built on a brutal lie.

While these cases typically focus on fake investments in cryptocurrency, sometimes the commodity is precious metals.

Cryptocurrency Kiosk Scams

AARP has seen an alarming increase in criminals using cryptocurrency kiosks to steal hardworking Americans' money. Cryptocurrency kiosks, also known as "crypto ATMs," "BTMs," or "virtual currency kiosks," can be found in supermarkets, convenience stores, gas stations, bars, and restaurants. Crypto kiosks allow people to conduct legitimate cryptocurrency transactions, such as sending money to digital wallets. Today, there are more than 30,000 crypto

kiosks nationwide. However, because crypto kiosks are largely unregulated at the state level compared to traditional financial institutions, such as banks and other money service businesses, they lack similar fraud protections. As a result, criminals are using them to steal hundreds of millions of dollars from Americans each year through fraudulent schemes.

The way these scams work is that criminals – often impersonating government officials or businesses – convince individuals that they must address an urgent financial matter, directing them to withdraw large amounts of cash and put that money into a crypto kiosk. It is then transferred to a digital wallet controlled by the criminal.

Older adults are disproportionately affected by fraud and scams using cryptocurrency kiosks. In the first eleven months of 2025, the FBI received reports of $333 million stolen in cryptocurrency kiosk scams. This is a significant increase from 2023, when the FBI received over 5,500 complaints involving crypto kiosks, and Americans reported over $189 million in stolen funds – and we know from FTC analysis that these figures represent just the tip of the iceberg. Additionally, over 65% of the theft losses in cryptocurrency kiosk fraud were experienced by adults 60+. AARP is advocating for important consumer protections that will deter criminals from leveraging cryptocurrency kiosks in their schemes. Our state-level advocacy has led to the passage of bills in 17 states to put important consumer protections in place, including fee and exchange rate transparency, fraud warnings, and transaction limits. This will help prevent older Americans from losing their retirement savings they worked so hard to amass.

A Path Forward

It may seem that we are in a fraud quagmire with little hope of getting out. There is no single solution, but there are roles for each sector of our society that will go a long way to turning the tide on the fraud tsunami.

For individuals, it's taking steps to better protect ourselves and our loved ones from fraud attacks. Such actions include freezing our credit, using a password manager and multifactor authentication, shredding documents, keeping our device operating systems updated to protect against known vulnerabilities and not engaging with incoming messages from unknown persons. And share what we know. Each of us should make it a point to talk about the latest we've heard about fraud with our family members and friends. The more we talk about these scams, the better protected we will be.

For educators, it is important that we tell consumers about the signs of the latest scams and their red flags. But what if we are able to come up with something simpler? If we can train our brains on how most scams come at us and what to do when they do, we could probably thwart a great deal of crime before it happens. Most scams come as a communication out of the blue that gets us immediately into a heightened emotional state and contains urgency. If we could train consumers that this scenario is likely a scam, we can train them how to react. AARP launched a campaign last summer that we call "Pause, Reflect, Protect" and we encourage others with fraud education campaigns to adopt the concept and the language.

Industry has a critical role to play as well. Financial institutions must continue to innovate on fraud controls and mitigation. Tech companies must build security into the design and manufacture of technology products, so that products come to market secure by design and safe by default.

From a public policy perspective, there are many actions Congress can take to address the fraud crisis.

For example, we are very pleased that Senators Gillibrand, Scott, and Britt introduced S.2544, the GUARD Act, which would direct federal funding to state and local law enforcement agencies to hire personnel, train staff, and secure tools to fight these crimes, empowering them to combat fraud committed against Americans. With new technology now playing a role in many forms of financial crime, law enforcement must have the right tools and training to unravel complex investigations and give victims the justice they deserve.

Senators Gillibrand, Scott, Kelly, and Moody have also introduced S.3355, the National Strategy for Combating Scams Act of 2025. This bipartisan legislation would bring together federal agencies, consumer advocates, and industry leaders to create a coordinated plan to fight scams. Amounts stolen from older adults is too often a life-altering amount, with significant and lasting impacts on older victims' financial security. By requiring collaboration across more than a dozen federal agencies, the bill helps cut through red tape, improve data sharing, and speed up enforcement when scams happen. It also makes sure the voices of those most affected—like older adults, survivors, and people with disabilities—are part of the solution. And importantly, it prioritizes making resources easier to access providing for more effective recovery for those who've been targeted.

AARP is also grateful to Senators Cornyn (R-TX) and Shaheen (D-NH), who introduced S.2950, the Scam Compound Accountability and Mobilization Act (SCAM Act). Many scams are perpetrated by transnational criminal organizations operating compounds overseas, with trafficked individuals coerced into defrauding Americans under duress. The SCAM Act will bring together federal agencies, law enforcement, and international partners to develop and implement a comprehensive strategy to counter scam compounds.

Finally, I would like to highlight H.R. 6426, the STOP Scams Against Seniors Act, which Representatives Amo (D-RI) and Shreve (R-IN) introduced. This legislation would empower state, local, and federal law enforcement agencies to better combat the growing epidemic of financial fraud targeting older Americans by authorizing federal Byrne JAG grants to support Elder Justice Task Forces nationwide, improving coordination and investigative capacity to pursue and prosecute criminals who exploit older adults.

AARP has also urged Congress to improve fraud reporting systems to ensure that law enforcement can adequately prioritize cases. The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) is the central site for reporting cyber-enabled crimes. Currently the FBI generally does not have advanced analytics capacity or interoperability across FBI systems. The result is that the FBI cannot identify commonalities between reported crimes and cannot search these reports to compare with information in other systems. Without the

ability to analyze information to identify the most commonly reported identifiers or between systems, the FBI cannot easily find potential links between cases. This leads to a situation in which the severity or extent of a crime is not recognized and not properly reviewed because it appears to be under a threshold for investigation. We are advocating for the FBI to prioritize enhancements to its data systems so that IC3 reports can be easily searchable and analyzed for potential links. This action, combined with support of the work of the National Elder Fraud Coordination Center to assist in intelligence gathering to bring light to links between cases, could greatly enhance law enforcement's successes in investigations and prosecutions of the criminals responsible for these crimes.

AARP is also advocating for the reinstatement of the casualty and theft loss deduction. The impact of fraud often goes beyond the theft of funds – if a criminal has stolen funds from a victim's 401(k) or other taxable account, this is considered a taxable event and the victim will likely owe taxes on the funds withdrawn from the account, and often end up in a higher tax bracket, compounding the loss. This an insurmountable burden for many victims, many of whom no longer have the ability to pay this tax bill due to the fraud loss. It can also impact a victim's eligibility for public benefits based on income. As of 2018, theft losses are no longer covered under the tax code and casualty losses are only covered if the loss is due to a major disaster as declared by a Presidential disaster declaration. There have been several pieces of legislation introduced in Congress to reinstate the casualty and theft loss deduction, including S.1773/H.R. 3469, the Tax Relief for Victims of Crimes, Scams, and Disasters Act, and AARP urges Congress to restore the deduction.

Industry and law enforcement should champion the success of the new National Elder Fraud Coordination Center (NEFCC), noted earlier. Even with underreporting, law enforcement is swimming in a sea of elder fraud reports. Scarce resources make it difficult for investigators to link cases. Jurisdictional challenges that come with transnational organized crime investigations limit prosecutions. Developing high-priority, high-impact cases takes time, labor, and analysis. A national coordination center like NEFCC -- with the leads, the data analysts, and the combined resources of the private and public sector -- can overcome these obstacles. In addition to the ability to create rich law enforcement investigative packages, incoming data from members could offer opportunities to neutralize known fraud vectors.

Indeed, in a commentary piece for *Fortune*, Nasdaq Chair and CEO Adena Friedman unveiled research that shows that annual GDP growth in the US would be 0.5% larger without fraud. Friedman says fraudulent acts too often go unnoticed but can be mitigated by better communication between the public and private sector. NEFCC marks an important and imminent means of producing this coordination.

Policymakers have an important role to help victims and bring the fight to fraud crime rings, including legislative solutions such as: providing more resources to train state and local law enforcement to investigate fraud crimes; reinstating the casualty loss deduction to address the significant tax burden that fraud victims face having to also pay taxes on the assets that were stolen; limiting the damage of fraud involving cryptocurrency kiosks; improving staffing of DOJ's Elder Justice Strike Forces; and enhanced efforts such as the National Elder Fraud

Coordination Center to bring the public and private sectors together to build cases for investigation and prosecution.

Conclusion

Addressing fraud requires more than piecemeal solutions; it demands a whole-of-society approach. We cannot educate our way out of the fraud crisis. Industry cannot mitigate and engineer our way out of it. Policymakers cannot regulate our way out of it. And law enforcement cannot arrest our way out of it.

But, together, educators, policymakers, law enforcement and industry can turn the tide against the vicious crime gangs who hold the power right now. Together, we can disrupt their business model, protect millions of consumers, and safeguard billions of dollars in savings and retirement accounts and in our economy.

We thank this Committee for bringing attention to this important issue and look forward to working with you to turn the tide on criminals committing fraud.

Chainalysis

Written Testimony of Jacqueline Burns Koven
Head of Cyber Threat Intelligence
Chainalysis Inc.

Before the
Senate Committee on Aging

Hearing on
Made in China, Paid by Seniors: Stopping the Surge of International Scams
January 14, 2026

Chairman Scott, Ranking Member Gillibrand, and distinguished members of the Special Committee: Thank you for inviting me to testify before you today on the pressing issue of international fraud and scams targeting older Americans, largely perpetrated by Chinese Organized Crime syndicates.

My name is Jacqueline Burns Koven, and I am the Head of Cyber Threat Intelligence for the blockchain data platform Chainalysis, where we harness the transparency of blockchains so that banks, businesses, and governments have the data and investigations, compliance, and security solutions they need for this new digital economy to thrive. We track cryptocurrency use by illicit actors, such as those carrying out investment and impersonation scams, and provide data on their financial activity to private- and public-sector customers, including the federal government.

In my testimony, I provide our assessment of the extent of scam activity and the role that cryptocurrencies play, and recommend how we can best mobilize and fight back against the growing scourge of scams that are putting all Americans, especially the most vulnerable among us, at risk. Once again, thank you for the opportunity to provide testimony on this important topic and continue to be a helpful partner on initiatives by Congress to better protect Americans – especially the most vulnerable – against scams and fraud.

Key Takeaways

- Cryptocurrencies are a primary channel for scammers' operations; with the right data, tools, and resources, this should put the government at an advantage.
- AI technology is making scams more effective, but it can also help detect fraud and prevent potential victims from falling victim to scams and sending money.
- Scammers are leveraging a vast, industrialized ecosystem of illicit tools and Chinese-language money laundering networks for their operations.
- Government and industry responses are fragmented and reactive. This crisis requires a unified and technology-enabled response.

Chainalysis

The growing intersection of scams and cryptocurrencies: $17B stolen in 2025

Americans, and especially older Americans, have not been immune to the threat posed by a global, organized, and pernicious scam industrial complex that adeptly leverages technological developments in social media, artificial intelligence, and cryptocurrencies.

Cryptocurrencies are often the financial rails of choice for scammers for the same reasons legitimate users use them – transactions are cross-border and instantaneous. But I am here today to emphasize that fraudsters' use of cryptocurrency should place them at a fundamental disadvantage, given the traceability and freezeability of many of these assets.

At Chainalysis, we analyze transaction data from blockchain networks in conjunction with open-source intelligence to map the ecosystem of legitimate and illicit flows. Our software provides a clear, visual representation of potential scam networks and laundering activities, a level of transparency that isn't possible for traditional forms of value transfer. Indeed, identifying a single cryptocurrency payment to a scam enterprise can often lead to identifying hundreds of other victim payments, the illicit services they leverage, and, in some cases, the scam compound from which the scammers operate. This visibility also enables us to estimate the amount of crypto funds stolen in fraud and scams over time.

According to Chainalysis data, 2025 was a record year for cryptocurrency scams, totalling an estimated $17 billion worth of cryptocurrency globally. Fraudsters can always be counted on to abuse novel technologies, and scam conglomerates are exceptionally adept at wielding new tools to scale their schemes to defraud Americans. Nobody is better than Chinese organized crime groups. They are the global market leaders in criminal fintech, and the Chinese-language underground ecosystem underpinning them is the most advanced in the world. They provide the entire spectrum of "crimeware" needed to conjure up a scam— social media profiles, mass calling and text spamming tools, stealer malware, data targeting lists with names and phone numbers of potential targets, AI technologies for deepfakes and voicecloning or fake investment platforms, laundering engines, and critical underground banking infrastructure – leveraging cryptocurrency as a form of payment.

The unique intelligence provided by the blockchain should be considered foundational for understanding the fraud problem at both a strategic and tactical level. The inherent transparency of blockchains, combined with the right data and tools, can illuminate the key components of the scam supply chain that support our national scam crisis. This can empower the U.S. Government to understand the scale of the problem, measure the impact of a counterscam strategy, surface investigative leads for the attribution of threat actors behind these campaigns, and identify opportunities for disruption.

Law enforcement and regulatory bodies can disrupt these networks, cut them off from the global financial system, and make it harder for them to profit by targeting illicit entities and networks on the

blockchain with sanctions and asset seizure. Blockchain analytics offers unique opportunities to trace illicit proceeds of crime, identify additional victims, and partner with the private sector to disrupt illicit networks and pursue restitution, rather than relying on one-off criminal investigations.

However, despite this huge potential for disruption, scammers are exploiting the disjointed, siloed nature of how the public and private sectors respond to their schemes. To be truly effective, we must pursue a multifaceted strategy that prioritizes uprooting the enabling scam infrastructure and identifying and bringing to justice the individuals responsible for perpetrating the scams.

Finally, we need to focus on prevention. AI-powered fraud prevention technology can stop victim funds from being stolen by scammers. But financial institutions and cryptocurrency businesses need guidance on when and how to intervene when they suspect their customers may be in the process of being scammed. On one hand, providing some friction may be critical to preventing funds from being sent to scammers. On the other hand, financial institutions may be hesitant to limit what their customers can do with their own money. Part of the solution involves using data to help financial institutions stop their customers from sending to likely scams at the point of transaction, rather than trying to anticipate what their customers are doing based on behavioral red flags alone. But even so, regulatory guidance on what these businesses can and cannot do to protect their customers is needed.

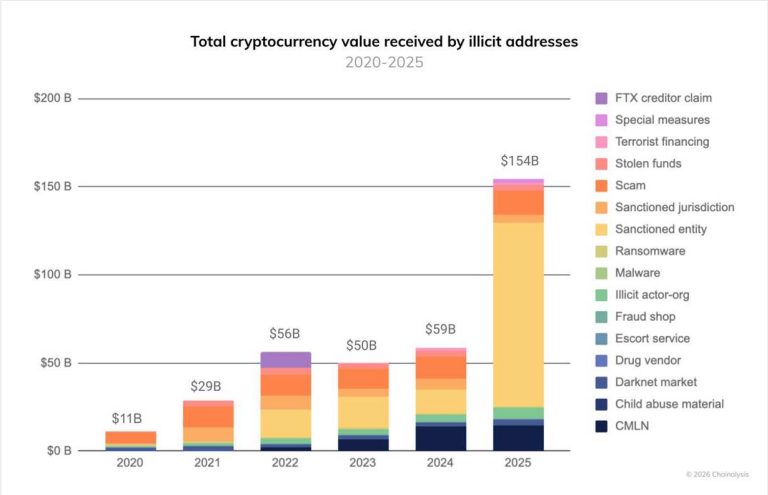
As such, our recommendations include:

1. Mobilize a whole-of-government and industry national anti-scam strategy that prioritizes enhanced reporting and collaborative information sharing that can best disrupt scam conglomerates;
2. Leverage technologies designed for both the prevention and remediation of scams;
3. Ensure financial institutions and crypto businesses are incentivized to assist in the prevention of transactions to scams and have appropriate guidance to enable them to do so;
4. Advocate to close gaps in the implementation of AML/CFT standards by FATF members, especially countries that scammers rely on to launder funds defrauded from Americans.

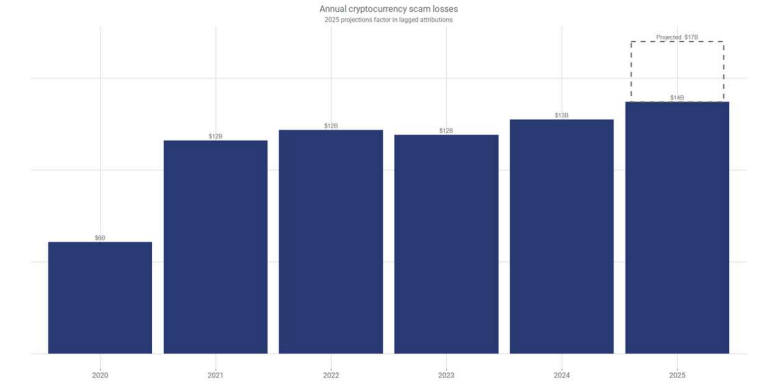
Chainalysis data and insights on scam activity

Chainalysis publishes an annual Crypto Crime Report that provides a detailed survey of the various types of illicit activity involving cryptocurrencies. In 2025, we estimate that the total amount of cryptocurrency received by illicit actors will be over $154 billion. This number will inevitably increase as we identify more illicit transactions associated with activity in 2025.

Chainalysis



In each of the past five years, scam operators received over $12 billion in cryptocurrency payments, and 2025 is estimated to be a record year for cryptocurrency scam revenue. Our data shows at least $14 billion worth of cryptocurrency scammed globally, and we expect that figure will exceed $17 billion as we retroactively identify more scams, based on historical trends.



Overall scam inflows have also surged, particularly through impersonation tactics that saw a staggering 1400% year-over-year growth. While high-yield investment programs (HYIP) and pig butchering remain dominant categories by volume, we're seeing increasing convergence across scam types as fraudsters leverage AI, sophisticated SMS phishing services, and complex money laundering networks to target victims more effectively than ever before.

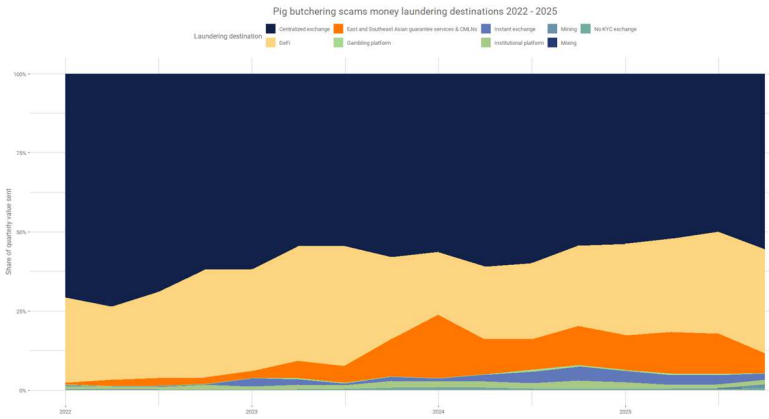
These tools and services underpinning all manner of scams are paid for with cryptocurrency, including the mass text phishing scam impersonating E-ZPass that targeted millions of Americans in 2025. To pull this off, the Chinese Smishing Triad leveraged software from “Lighthouse,” a Chinese-language vendor on Telegram that accepts cryptocurrency in exchange for "phishing for dummies" with hundreds of templates for fake websites, domain setup tools, and features designed to evade detection. The scale of Lighthouse phishing attacks is staggering. In 20 days, approximately 200,000 fraudulent websites created using Lighthouse were used to attract 'well over 1,000,000 potential victims' in at least 121 countries.

Human trafficking is also behind some of the most pernicious scams. Chainalysis collaborates with Non-Governmental Organizations such as the International Justice Mission, which operates in the world’s corruption hotspots, including the Golden Triangle, enabling Chainalysis to identify cryptocurrency wallets belonging to crime syndicates operating within specific compounds. These wallets tell of the horrors not only of the scam victims themselves but of the estimated hundreds of thousands of human trafficking victims behind the scam compounds. Chainalysis has previously detailed how we have traced a single ransom payment in cryptocurrency made by a trafficking victim held captive in the KK Park compound in Myanmar to a centralized wallet commingled with hundreds of millions of dollars in scam

proceeds. We've now identified cryptocurrency wallets belonging to compounds across multiple countries and continents.

The International threat: Scam laundering leverages offshore exchanges and Chinese-language money laundering services, with a strong regional nexus to East and Southeast Asia

We not only track the amount of cryptocurrency funds received by scam operators but also where those funds are directed for purposes of laundering or cashing out to fiat currency. In the last few years, centralized exchanges (CEXs) have been the primary destinations for laundering funds from scams; however, Decentralized Exchanges and Chinese Money Laundering Networks (CMLNs) have seen increased adoption among scammers. The regional connection of the scamming syndicates is evidenced by the off-ramping patterns we observe, with a significant portion of the proceeds from pig butchering scams flowing to CMLNs. It is important to note that scam proceeds are largely laundered through overseas entities, reinforcing the effectiveness of the US anti-money laundering regime domestically.

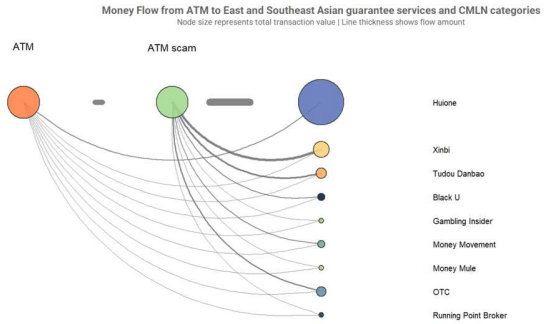


In recent years, CLMNs have emerged as dominant channels for laundering illicit cryptocurrency, including funds stolen through fraud and scams. Guarantee services operate as one-stop shops for illicit actors needing the technology, infrastructure, and resources to conduct scams. They function primarily as marketing venues and escrow infrastructure for these networks. While they provide trust mechanisms for vendors, they don't control the underlying laundering activity. Huione and Xinbi have dominated the market for the past few years, and many other guarantee services continue to operate freely. Many merchants on these platforms put little effort into masking their illicit activities, advertising

the types of services they offer using thinly veiled code words. They openly cater to the scam ecosystem by providing technology for facial recognition or facial alteration, targeted data lists for outreach to potential victims, web hosting services, social media accounts and content creation, orchestration of pig butchering and Ponzi schemes, and global passports, visas, and purportedly assisting with applications, and AI software.

Our on-chain analysis continues to show persistent connections between cryptocurrency scams and operations based in East and Southeast Asia. While the Huione Guarantee platform identified in our 2025 report was effectively shut down following FinCEN's 311 designation — which severed its access to the U.S. financial system — we've observed expansion of similar operations across the region.

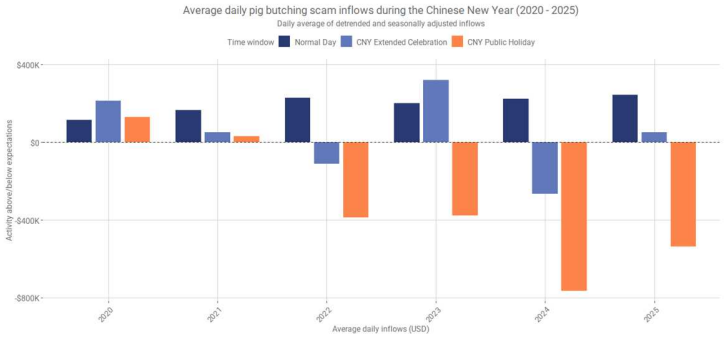
Our analysis reveals that funds originating at U.S. crypto ATMs frequently flow into wallets associated with Southeast Asia-based CMLNs and guarantee services, which serve as key intermediaries in the broader global scam infrastructure. While not all on-chain flows from scams to CMLNs can be traced directly to ATM on-ramps, crypto ATMs remain a critical input for scammers targeting older adults, who are often instructed to convert cash into cryptocurrency at these kiosks before funds are quickly transferred. In this context, actors leveraging crypto ATMs as both payment conduits and loci of fraud increasingly depend on CMLNs to launder and integrate stolen funds into the wider financial system, illustrating how traditional elder fraud has evolved into a transnational, crypto-enabled ecosystem.



Stronger state protections that require owners and operators of crypto kiosks to set transaction limits, inform users of risks, provide receipts, and refund qualifying payments could help prevent older adults from falling prey to certain scams.

The chart below shows the centrality of Southeast Asia to pig butchering scams by examining the 'holiday effect' associated with the Chinese New Year public holiday (7 days at the start of the 15-day

new year celebration). Starting around 2022, roughly when Huione began to play a central role in laundering funds from scam compounds such as KK Park, there was a notable reduction in pig butchering scam activity during the 7-day public holiday associated with the Chinese New Year. After the data have been detrended and seasonally adjusted, average daily pig butchering activity drops notably during these short windows. This pattern suggests that the Chinese holiday is associated with a reduction in inflows to pig butchering scams, indicating that actors in East and Southeast Asia play an important role in this scam ecosystem.



Recent enforcement actions against overseas money laundering facilitation networks, including sanctions designations and advisories, have shed light on the national security threat that impacts victims worldwide. These actions include the designation of the Prince Group by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and the Office of Financial Sanctions Implementation (OFSI) by HM Treasury in the UK, the Financial Crimes Enforcement Network (FinCEN)'s Final Rule designating Huione Group as a primary money laundering concern, and FinCEN's advisory on Chinese money laundering networks.

We applaud these actions, but the threat actors are resilient. As with other genres of illicit on-chain activity, actions against guarantee services can be disruptive, but the core networks persist and migrate to alternative channels when challenged. While Huione's guarantee operations were disrupted after Telegram removed some of their accounts, vendors using Huione have continued to use or advertise on alternative platforms, their operations largely uninterrupted. While these hubs continue to connect vendors and buyers, most vendors promote advertisements across platforms and are not reliant on any specific service. As with legitimate e-commerce platforms, service ratings and reviews create accountability within the illicit ecosystem, and vendors often cultivate their market reputation through public attestations of their reliability and service quality.

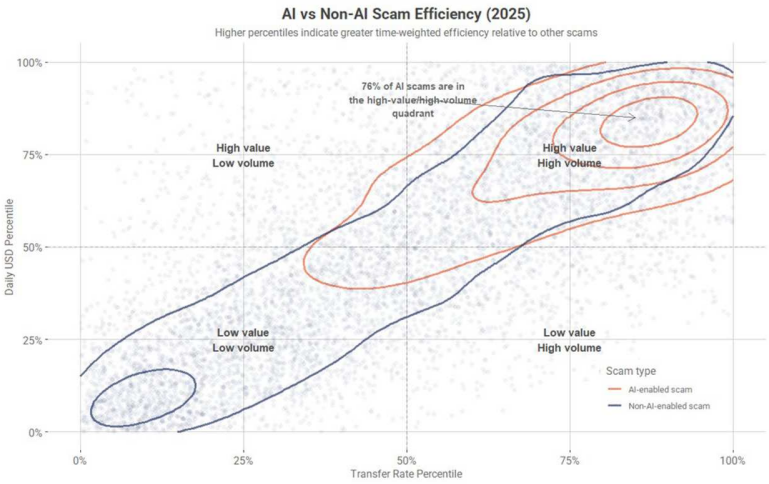
The Local Impact: Elderly US citizens are uniquely vulnerable to the threat of scams, and the role that cryptocurrency can play

Scams targeting older adults represent some of the most financially devastating frauds reported in the US. Recent estimates indicate that Americans aged 60 and older lose billions of dollars annually to financial exploitation and fraud, including nearly $4.9 billion in reported losses in 2024 alone, more than any other age group, according to AARP and FBI data. The FBI's Internet Crime Complaint Center (IC3) further underscores this trend: in 2024, individuals aged 60 and older reported $2.8 billion in losses from crypto-related scams, reflecting both the scale and the growing role of digital assets in modern fraud. While elder fraud encompasses a broad range of schemes, cryptocurrency ATMs have emerged as a notable on-ramp for scams. Reported losses from Bitcoin ATM fraud have risen sharply in recent years, and older victims are disproportionately affected by these kiosk-based conversions. The elderly, who often have significant retirement savings yet limited familiarity with irreversible digital payment methods, remain particularly vulnerable to such tactics.

AI and professional scamming tools increase scam severity

While generative AI can accelerate legitimate innovation, it can also make scams more scalable and affordable for bad actors. We are rapidly moving toward a future in which virtually all scams will incorporate AI into their operations to some degree. While many scams involve buying AI tools through traditional payment channels, a significant subset buys these tools on-chain, making their transactions visible. Exploring the differences between scams with visible on-chain associations to Chinese AI vendors lets us probe the scale and efficiency of AI.

As depicted below, 76% of AI scams are in the time-weighted high-value/high-volume quadrant. This means that a large majority of scams with demonstrable on-chain links to often Telegram-based Chinese AI vendors selling face-swap software, deepfake technologies, and LLMs tend to (1) scale more quickly (i.e., higher incoming transfer rates) and (2) be more severe (i.e., higher daily USD volumes) than scams without these clear on-chain links to AI vendors.



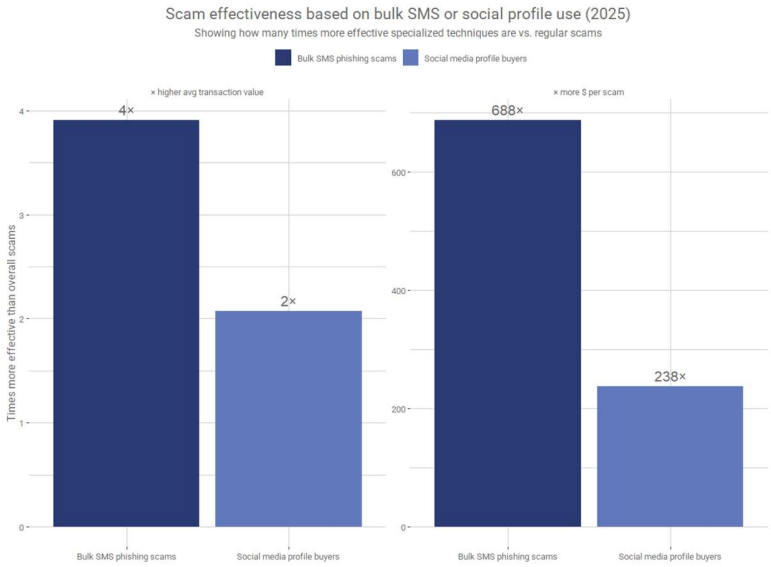
Our analysis reveals that, on average, scams with on-chain links to AI vendors extract $3.2 million per operation compared to $719,000 for those without an on-chain link — 4.5 times more revenue per scam. These AI-related operations also demonstrate significantly greater time-weighed efficiency:

- Higher daily revenue: $4,838 vs $518 median daily revenue
- Increased transaction volume: 35.1 vs 3.89 average transfers per day (9x more transaction activity)

These metrics suggest both higher operational efficiency and potentially broader victim reach. The increased transaction volume indicates that AI is enabling scammers to reach and manage more victims simultaneously, a trend consistent with the industrialization of fraud. In contrast, the increased scam volume suggests that AI is likewise making the larger scams more persuasive.

The professionalization of scamming tools is also a force multiplier to execute industrial-scale scams. Many of these campaigns have a social media angle, given that such platforms provide access to millions of users, and are thus prime targets for sending automated messages. In such cases, scammers may buy bulk social media profiles and use SMS and phishing kits to communicate. Scams leveraging these phishing kits are 688 times more effective in dollar terms and four times more effective in average transaction size than regular scams. Scams that buy bulk social media accounts are likewise 238 times

more effective in dollar terms and two times more effective in average transaction value than regular scams.



Chainalysis data and tools as part of the response

The uniquely transparent manner in which blockchains operate opens up powerful opportunities to gain insights into illicit activity occurring on these networks. However, this data is difficult to access without the right tools, training, and data. Over the past ten years, Chainalysis has become indispensable to the workflows of law enforcement and intelligence agencies in the US and globally, as well as to corporate compliance and risk departments.

The most demonstrable result from this work is the support that Chainalysis has provided on hundreds of cryptocurrency cases since its inception, involving seizures and freezing of assets in partnership with

government agencies worldwide, helping secure an estimated $34 billion dollars worth of illicit crypto.[1] 2025 saw unprecedented law enforcement action against scams, including two of the largest-ever crypto-related law enforcement actions directly connected to scam operations.

The following notable scam-related crypto seizures were only possible due to the transparency of the blockchain and the availability of state-of-the-art tools and data like those Chainalysis provides. These actions mark a shift from reactive victim recovery to systematic dismantling, targeting not just front-line scammers, but also the executives, infrastructure, shell companies, and financial rails that sustain them. Together, they illustrate a new, more integrated phase in scam enforcement: one focused on breaking the economic backbone of crypto-enabled fraud at scale and across borders, rather than treating scams as local, isolated, or purely digital crimes.

- In October 2025, the U.S. Department of Justice unsealed charges against a Cambodian national and Prince Group chairman Chen Zhi for allegedly overseeing Cambodian forced-labor scam compounds that powered large-scale cryptocurrency fraud targeting victims worldwide. According to prosecutors, these compounds operated as vertically integrated fraud factories: trafficked individuals were coerced into running pig butchering investment scams and romance fraud schemes, laundering proceeds through cryptocurrency to obscure attribution and scale operations globally. Critically, U.S. authorities paired these indictments with large-scale financial disruption, including arrests across transnational money laundering networks and actions to seize and forfeit more than $15 billion in illicit proceeds linked to scam activity.
- In November 2025, the UK's Metropolitan Police secured convictions in a landmark crypto money laundering case that led to the world's largest confirmed cryptocurrency seizure, recovering over 61,000 Bitcoin — currently valued at around £5 billion — from Chinese national Zhimin Qian (also known as Yadi Zhang), who orchestrated a multibillion-pound investment fraud in China that victimized more than 128,000 people between 2014 and 2017.
- Also in November 2025, the U.S. Scam Center Strike Force's success in seizing over $401 million in cryptocurrency demonstrates the effectiveness of blockchain intelligence in taking action against transnational scam operations.
- In August 2025, it was revealed that APAC-based law enforcement froze $47 million in pig butchering funds through collaboration with the private sector, following a similarly successful public-private sector collaboration that resulted in the freeze of $225 million in funds.

AML compliance and the need for prevention

[1] "Asset Seizure and Cryptocurrency: How Chainalysis Creates Opportunities for Self-Sustaining Law Enforcement," *Chainalysis*, Mar. 26, 2025, https://www.chainalysis.com/blog/cryptocurrency-asset-seizure/.

Chainalysis

Chainalysis data and tools are not only integral to public sector operations and seizures but also play an important role in the AML programs of financial institutions, crypto businesses, and a broad swath of private sector businesses motivated to stop scam activity. Chainalysis data is leveraged by cryptocurrency businesses and financial institutions for transaction monitoring, enhanced due diligence, and, when appropriate, enhancing SAR filings.

At Chainalysis, we also think it is imperative to move beyond reactive compliance and fraud workflows and to develop processes to prevent Americans from falling prey to scams altogether. Furthermore, in the same way that we observe criminals adapt to and leverage technological developments to their own ends, so too can we harness and encourage the use of AI technology to help financial institutions and crypto platforms prevent their customers from sending funds to likely scams.

Chainalysis Alterya provides real-time proactive fraud protection for payments and enhanced fraud detection during KYC for exchanges, blockchains, and wallet providers. Alterya has already helped top crypto exchanges decrease fraud by up to 60%, reduce scam-related disputes, and improve the efficiency of manual operations. Alterya utilizes artificial intelligence and other advanced techniques to identify scam activities across various online sources, enabling large-scale early "upstream" detection. We construct a comprehensive scam social graph that interconnects fraudulent activities across multiple platforms, payment systems, and blockchains. Our adversaries are leveraging AI to rob Americans of their life savings, and we must leverage that very technology to beat them at their own game.

Alterya monitors $23B+ in monthly transactions and helps protect hundreds of millions of users across crypto and fiat payment rails, focusing on recipient-side risk and money-mule detection, critical for stopping authorized push-payment (APP) fraud, where victims are socially engineered into authorizing transfers from their own accounts to criminals. Over the past 12 months, Alterya has prevented more than $300 million in losses by supporting customers in proactively reducing fraud. This is what the future of combating scams looks like.

Recommendations

We are encouraged that this Committee is considering ways to strengthen the U.S. response to scams and fraud involving cryptocurrency that target older victims. We suggest a multi-pronged approach to address this complex problem, consisting of four key recommendations:

1. Mobilize a whole-of-government and industry national anti-scam strategy that prioritizes enhanced reporting and collaborative information sharing that can best disrupt scam conglomerates;
2. Leverage technologies designed for both the prevention and remediation of scams;
3. Ensure financial institutions and crypto businesses are incentivized to assist in the prevention of transactions to scams and have appropriate guidance to enable them to do so;

4. Advocate to close gaps in the implementation of AML/CFT standards by FATF members, especially countries that scammers rely on to launder funds defrauded from Americans.

Taken together and properly implemented, these recommendations will help limit financial flows to scammers, either by preventing victims from sending funds in the first place or by dismantling the scam operations themselves. Further details on each of these are provided below:

1. **Create a national anti-scam strategy to orchestrate a comprehensive response which includes centralizing U.S. victim scam reporting, streamlining coordinated action to dismantle scam conglomerates and return funds to victims, and facilitating information sharing between the public and private sectors.**

i. Improved reporting mechanisms

Today, scam victims in America have multiple options for reporting their crimes to federal and local law enforcement. This is one factor contributing to a fragmented approach to combating scams and has hindered our response time and visibility into the true scale of the impact on potential victims, both in the US and abroad.

A centralized reporting database that feeds from state, local, and federal sources is critical to enhancing efficiency and actionable intelligence for cases that lead to the recovery of funds, restitution, and the prevention of additional victims. National coordination could streamline the process of connecting a single victim to a larger scheme that has netted thousands of victims and millions of dollars in funds, optimizing opportunities for disruption, the prospect of returning seized assets to victims, and making scammers less profitable overall. Similarly, Suspicious Activity Reports (SARs) are filed by financial institutions, but the crucial information contained in these reports about specific scams is not accessible to other financial institutions or to entities supporting scam prevention. This lack of information sharing creates blind spots and delays in response, enabling scammers to continue their illicit activities unabated.

ii. Prioritizing information sharing and collaboration

Addressing the challenge of crypto-integrated laundering networks demands a coordinated public-private partnership and a paradigm shift from reactive enforcement against individual platforms to proactive disruption of the underlying networks. By combining law enforcement's legal authorities with the private sector's technical capabilities and blockchain analytics expertise, the industry can more effectively identify and dismantle these services operating across multiple platforms, jurisdictions, and communication channels. On-chain transparency provides unprecedented visibility into these operations, enabling stakeholders to assess the cost and risk of operating large-scale money laundering services. Future intervention strategies must prioritize this collaborative approach to achieve

meaningful, lasting disruption of crypto-integrated laundering networks, including Chinese-language money-laundering operations.

Public-private partnerships are already having success. Chainalysis's Operation Spincaster program was designed to disrupt and prevent scams through public-private collaboration by proactively identifying thousands of compromised wallets.[2] This actionable intelligence formed the basis for a series of operational sprints across six countries, including 19 public-sector agencies and 18 crypto exchanges. Over 7,000 leads were disseminated during these sprints relating to approximately USD $187 million of losses. These leads were used to close accounts, seize funds, and build intelligence to prevent future scams.

Further, Chainalysis is a member of the National Elder Fraud Coordination Center, the first-ever national effort that analyzes and assembles private and public sector data and resources into the investigative packages needed by law enforcement to investigate and prosecute criminal fraud rings targeting older Americans. These are examples of how formalized efforts to streamline private-public collaboration can optimize outcomes.

Singapore's Anti-Scam Command (ASCom) serves as a potential model for efficiently combating scams by eliminating silos and working constructively with over 80 private-sector partners. The industry and regulatory bodies must work together to break down these information silos and adopt a more cohesive, collaborative approach to combating cryptocurrency-related scams. This will ensure that the inherent advantages of blockchain technology for tracing and combating financial crime are fully leveraged and that scammers cannot exploit the system due to gaps in communication and information sharing.

The recently announced Scam Center Strike Force and proposed legislation, such as the Scam Compound Accountability and Mobilization Act, will help define and execute an international strategy to take on scam compounds globally. This approach should study the scam supply chain holistically and leverage all levers of government, including law enforcement and regulatory actions, to target the entire scam supply chain, from money launderers to gambling syndicates to compounds to phishing kit developers to data brokers.

2. **Encourage the adoption of advanced technologies to combat scammers' growing sophistication and to prevent and remediate scams across fiat and digital asset rails.**

i. Broaden access to data, tools, and training

[2] "Introducing Chainalysis Operation Spincaster: An Ecosystem-Wide Initiative To Disrupt and Prevent Billions in Losses to Crypto Scams," *Chainalysis*, Jul. 18, 2024, https://www.chainalysis.com/blog/operation-spincaster/.

With the broader adoption of cryptocurrency on the rise, including among illicit actors, it is no longer sufficient to confine knowledge of crypto networks to a small group of technical experts. Rather, government agencies and departments must have the resources to ensure that a broad spectrum of personnel receive the latest training on how crypto networks operate, how blockchain analysis can supplement traditional analytical and operational workflows, and what actions can be taken to quickly disrupt illicit fund movements through crypto networks. Too often, victims are turned away from local authorities who are ill-equipped or even uninformed as to how to take on crypto cases. Other times, an individual complaint might not be prioritized if law enforcement doesn't have the analytic tools it needs to connect a low-value scam payment to a larger scam conglomerate that nets tens or hundreds of millions of dollars. Furthermore, we must acknowledge that a significant number of scams likely go unreported; however, the transparent nature of the blockchain enables investigators to identify all potential victim payments into a scam and can vastly expand their case with assistance from cryptocurrency businesses.

While the proposed Guarding Unprotected Aging Retirees from Deception (GUARD) Act would expressly allow federal law enforcement agencies to assist in these cases, we believe this should not replace providing tools and training to state and local agencies so they can help victims in their jurisdictions.

Particular offices within agencies have invested in integrating blockchain analytics into their workflows and achieved significant success, among them IRS Criminal Investigations and the FBI's Virtual Asset Unit. However, the extensive overlap of crypto across many agencies' missions necessitates a broader cohort of agencies and their staff to understand the underlying technology, have access to the same tools, and receive training to encourage more successful outcomes.

ii. Adoption of cutting-edge technology, systems, and tools that move beyond reactive enforcement

While the traditional reactive paradigm of enforcement is important, it is not enough for the speed and scale of scams today. The organized crime groups behind scams move quickly and operate in regions that are difficult to access, making real-time prevention mechanisms a vital line of defense. Given these challenges and the sheer volume of victims, some agencies and investigators across the public and private sectors are now turning to advanced proactive detection techniques.

The future of fraud prevention relies on the deployment of novel technologies such as machine learning and AI. Chainalysis Alterya provides financial institutions with the tools to map the entire lifecycle of fraudulent operations, from initial online scam campaigns and money muling to monetization within financial services and subsequent money laundering and cash-out processes through proactive AI-driven solutions. It identifies scammers before they meet their victims, collecting identifying information about the scammers and the fraudulent scheme. This data is then integrated with customers' transaction-

monitoring platforms, providing real-time analysis of scam exposure and enabling them to identify and track interactions with scam addresses, assess risk, and take preventive measures.

All relevant agencies and law enforcement should also have this opportunity to move decisively upstream and take the fight directly to scammers. In such a scenario, rather than simply investigating reported crimes, the public and private sectors could best leverage real-time blockchain data, DNS data, and AI technology to identify, disrupt, and potentially prevent illicit activity.

For example, Chainalysis Alterya can help agencies transform scattered victim reports into mapped scam campaigns that connect wallets, domains, social accounts, and other identifiers, giving agencies a single source of truth on how a fraud network actually operates. That same network view becomes the foundation for case triage and victim support—analysts can quickly see which victims are linked, what other identifiers to pursue, and where to prioritize investigative resources. This network view can also power supervisory analytics and market-wide disruption, enabling agencies to track typologies over time, measure exposure across institutions and rails, and coordinate targeted interventions against the scamming infrastructure that makes these frauds possible in the first place.

Congress should ensure that relevant federal, state, and local agencies have the tools, resources, and legal authorities necessary to: (1) access, analyze, and act on blockchain and other digital intelligence; (2) collaborate effectively with financial institutions, crypto platforms, and other private-sector intermediaries; and (3) integrate AI-enabled risk detection into their investigative, supervisory, and consumer protection workflows. This combination of AI-driven analytics and blockchain intelligence can materially improve our ability to detect, disrupt, and deter scams at scale, while strengthening restitution outcomes for victims and raising the cost of doing business for organized scam networks.

3. **Provide guidance to financial institutions and crypto businesses to help them prevent customers from sending funds to scams and intervene when scam-detection technology identifies risk.**

Although the technology exists for cryptocurrency businesses and financial institutions to detect when a customer is trying to send funds to a scam wallet, they lack the legal basis to hold a customer's funds. Even after a crypto business warns a customer that they are trying to send funds to a scam, more often than not, the customer is so duped by the scammers that they will still opt to release their funds to the scammer. The U.S. Government should establish clear, consistent guidelines for how financial institutions and cryptocurrency businesses may intervene when they suspect customers are being targeted by scams, so that firms are not forced to choose between overreaching into consumers' access to their own funds and passively facilitating payments into organized scam networks.

Today, banks and crypto platforms lack standardized expectations and a legal basis around when and how they can slow, block, or scrutinize suspicious transactions, and what forms of customer outreach and friction are appropriate in these scenarios. With better access to data, typologies, and public-private

information sharing, these institutions would be far better equipped to strike the right balance between consumer protection and customer autonomy. Congress should therefore direct regulators to issue guidance that encourages the use of advanced fraud-prevention technologies, such as Chainalysis Alterya, which enable financial institutions and cryptocurrency businesses to detect and prevent likely scam payments in real time. These tools have already demonstrated that they can significantly reduce authorized push payment (APP) fraud losses, lower the volume of customer disputes, and help institutions retain customers by protecting them from devastating financial harm while preserving safe access to their own money.

One solution could be to implement an optional, scams-specific hold on funds, backed by liability protections, that allows stablecoin issuers, cryptocurrency businesses, and financial institutions to temporarily stop suspicious transactions as soon as they or law enforcement identify red flags.

4. **Close gaps in AML/CFT standards implementation for FATF members, especially countries that host scam compounds and the services they rely on to launder funds defrauded from Americans.**

   More capacity building is needed in jurisdictions with weak AML and CFT policies – particularly across Southeast Asia, where scam compounds operated by Chinese transnational criminal organizations and their local partners have become major hubs for large-scale fraud targeting Americans and other victims worldwide. These same networks increasingly rely on Chinese-language money laundering services as key vehicles for laundering the proceeds of these schemes and cycling them back into the global financial system. In the absence of cooperation, more pressure is needed to disrupt the financial networks and the digital asset services flagrantly abusing laws and regulatory norms. Sanctions have proven to be an effective tool, and sustained enforcement actions targeting every facet of the scam supply chain – especially the offshore institutions that defy international norms and AML/CFT processes and standards – would help cut off scam perpetrators and their facilitators from the global financial system.

United States Government Accountability Office

Testimony

Before the Special Committee on Aging, U.S. Senate

For Release on Delivery
Expected at 3:30 p.m. ET
Wednesday, January 14, 2026

CONSUMER PROTECTION

Expeditious Actions Needed to Implement a Government-wide Strategy and Related Efforts to Counter Scams

Statement of Seto J. Bagdoyan, Director,
Forensic Audits and Investigative Service

GAO-26-108842

GAO Highlights

CONSUMER PROTECTION

Expeditious Actions Needed to Implement a Government-wide Strategy and Related Efforts to Counter Scams

GAO-26-108842 January 14, 2026

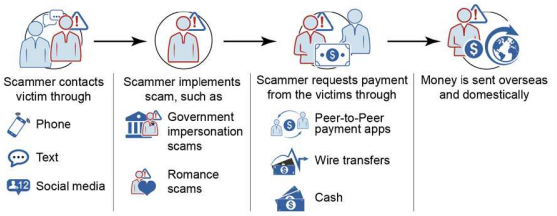
A testimony before the Special Committee on Aging, U.S. Senate

For more information, contact: Seto J. Bagdoyan at BagdoyanS@gao.gov

What GAO Found

Scams occur in a variety of forms and are a growing risk to consumers.

Examples of a Scam Execution Process



Sources: GAO analysis of publicly available information on scams, including from the Federal Trade Commission and Federal Bureau of Investigation; Icons-Studio, sdecoret/stock.adobe.com, GAO (icons). | GAO-26-108842

Note: Other types of contact methods, scams, and payment methods exist.

At least 13 federal agencies engage in a range of activities related to countering scams. The agency activities cover a spectrum of roles intended to prevent, detect, and respond to scams. However, each agency largely carries out these activities independently. None of the 13 federal agencies that GAO spoke with were aware of a government-wide strategy to guide efforts to combat scams, nor did GAO independently identify such a strategy. In its April 2025 report, GAO recommended that the Federal Bureau of Investigation (FBI) lead a federal effort, in collaboration with other agencies, to develop and implement a government-wide strategy to counter scams and coordinate related activities. The FBI recently outlined actions to address this recommendation.

The Consumer Protection Financial Bureau (CFPB), the FBI, and the Federal Trade Commission (FTC) collect and report on consumer complaints both directly and from other agencies. Data limitations prevent agencies from determining a total number of scam complaints and financial losses. Accordingly, 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. A government-wide estimate would capture the scale of scams, and a common definition is necessary for producing such an estimate and for developing a government-wide strategy.

In its April 2025 report, GAO made separate recommendations to CFPB, the FBI, and FTC to (1) develop a common definition of scams, (2) harmonize data collection, (3) report an estimate of the number of scam complaints each receives and (4) produce a single, government-wide estimate of the number of consumers affected by scams. In a recent update, the FBI and FTC outlined various concerns with these recommendations, such as differing authorities and mandates among agencies. However, GAO maintains that these recommendations remain valid. In October 2025, CFPB stated that it will monitor FBI and FTC actions before determining if any actions of its own are warranted.

Why GAO Did This Study

Scams, a method of committing fraud, involve the use of deception or manipulation intended to achieve financial gain. Scams often cause individual victims to lose large sums—in some cases their entire life savings. Federal agencies such as the FBI and FTC have responsibilities that include preventing and responding to scams against Americans.

This statement discusses (1) federal agencies' activities to prevent and respond to scams and the need for a comprehensive, government-wide strategy to guide their efforts and (2) federal agencies' activities to compile scam-related consumer-complaint data and estimate the total number of scams and related financial losses. It also provides updates on the status of 3 agencies' actions to address applicable recommendations.

This statement is based on GAO's April 2025 report on federal efforts to combat scams (GAO-25-107088). For that report, GAO analyzed publicly available information (including prior GAO reports) and relevant agency documents. GAO also interviewed officials from 13 different federal agencies involved in countering scams.

What GAO Recommends

In April 2025 GAO made 16 total recommendations to CFPB, the FBI, and FTC. The FBI disagreed with three recommendations, including those related to the development of a government-wide estimate and a definition of scams. FTC neither agreed nor disagreed with the five recommendations made to it. CFPB did not respond with comments. The agencies' responses to certain recommendations are discussed in this statement.

Chairman Scott, Ranking Member Gillibrand, and Members of the Committee:

I am pleased to appear before you today to discuss findings from our April 2025 report on scams that target consumers, including older adults, and the various ways federal agencies counter such scams.[1] Scams, a method of committing fraud, involve the use of deception or manipulation intended to achieve financial gain for the scammer. In perpetrating various scams, scammers deceive victims into making a payment or providing information to make a payment to benefit the scammer. These payments are often made via Peer-2-Peer (P2P) payment applications, gift cards, and wire transfers.[2] In addition to inflicting emotional distress, scams have caused individual victims to lose tens of thousands of dollars, and, in some cases, their entire life savings.

Criminal organizations operating throughout the country and world use thousands of scammers to target victims and induce them into giving them their money under false pretenses. According to the United Nations, these organized crime groups continue to expand their operations and increase the sophistication of scams.[3]

A single example highlights the scope and reach of scams. A 2023 international police operation against online financial crime, including scams, concluded with over 3,000 arrests and the seizure of $300 million

[1]GAO, *Consumer Protection: Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams*, GAO-25-107088 (Washington, D.C.: Apr. 8, 2025). This statement refers to persons 60 and older when using the term "older adults." This definition is consistent with the requirements in Section 2(1) of the Elder Abuse Prevention and Prosecution Act, which references Section 2011 of the Social Security Act (42 U.S.C. 1397j(5)) (defining "elder" as an individual age 60 or older).

[2]P2P payment applications allow consumers to send and receive money from mobile devices through a linked bank account. A gift card is a plastic card or other payment code or device that is purchased on a prepaid basis; issued at a specific amount; and redeemable at a single merchant or an affiliated group of merchants that share the same name, mark, or logo. A wire transfer is a way to send money electronically to a domestic or an international recipient.

[3]United Nations Office on Drugs and Crime, *Casinos, cyber fraud, and trafficking in persons for forced Criminality in Southeast Asia* (September 2023), https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf.

worth of assets across 34 countries, including the United States.[4] Within the United States, the Department of Justice (DOJ) has also identified the involvement of transnational criminal organizations that have taken tens of millions of dollars from Americans through scams.

My remarks today summarize findings from our April 2025 report that are of particular interest to the Committee for purposes of this hearing. Specifically, I will describe our findings related to:

1. federal agencies' activities to prevent and respond to scams and the need for a comprehensive, government-wide strategy to guide their efforts, as well as the status of agencies' actions to address our applicable recommendations.
2. federal agencies' activities to compile scam-related consumer-complaint data and estimate the total number of scams and related financial losses, as well as the status of agencies' actions to address our applicable recommendations.

Detailed information on the objectives, scope, and methodology for this work can be found in our April 2025 report.[5] In addition, for this statement we summarize information recently provided by federal agencies in October and November 2025 on the status of actions they have taken or planned in response to our April 2025 recommendations.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Several federal agencies play a role in preventing and responding to scams including:

- Consumer Financial Protection Bureau (CFPB),

[4]Interpol, *USD 300 million seized and 3,500 suspects arrested in international financial crime operation* (Dec. 19, 2023), https://www.interpol.int/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation.

[5]GAO-25-107088.

- the Federal Bureau of Investigation (FBI) and the Executive Office for United States Attorneys (within the DOJ),
- the Federal Trade Commission (FTC) and
- the Department of the Treasury.[6]

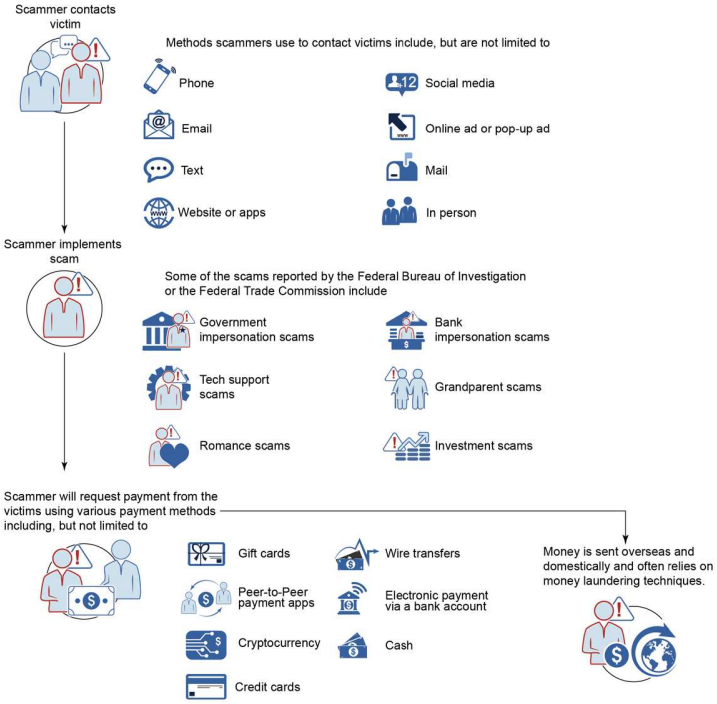
Scams involving the use of information technology have been around for decades. In an early common scheme, text messages were sent to individuals requesting that funds be sent to someone purporting to be a family member.

According to our analysis of publicly available information, scams today can occur in different forms. Scams involve a scammer contacting the victim, through means such as text message or social media; engaging the victim with a particular scam scheme; and requesting a payment, such as a wire transfer, for a false purpose. Figure 1 illustrates how scams may generally be carried out.

[6]For the full list of the 13 federal agencies we identified as playing a role in preventing and responding to scams, see GAO-25-107088.

Figure 1: Common Examples of the Scam Execution Process

Scams can be carried out by individuals and bad actors, including criminal networks operating both outside the United States and domestically.



Sources: GAO analysis of publicly available information on scams, including from the Federal Trade Commission and Federal Bureau of Investigation; Icons-Studio, sdecoret/stock.adobe.com, GAO (icons). | GAO-26-108842

Figure 2: Examples of Scam Types

Types of scams

 **Government/business impersonation**	**Government/business impersonation scams** occur when the scammer fraudulently identifies as a government or business official to manipulate or steal from the victim.
 **Tech support**	**Tech support scams** occur when the scammer poses as technical or customer support/service. For example, the tech support scammer may trick an individual with a pop-up window that appears on the individual's computer that might look like an error message from the operating system. The pop-up window will direct the individual to call the tech support team. The scammer, pretending to be a tech support team member, will request money to provide assistance.
 **Grandparents**	**Grandparent scams** involve a scammer impersonating a family member, usually a grandchild, of an older adult or someone who says the family member is in trouble. The scammer claims that money is immediately needed to assist the family member.
 **Romance**	**Romance scams** occur when a scammer adopts a fake online identity to gain a victim's affection (romantic or platonic) and trust and then uses the illusion of a romantic or close relationship to manipulate or steal from the victim.
 **Investment**	**Investment scams** involve a scammer offering low- or no-risk investments, guaranteed returns, overly consistent returns, complex strategies, or unregistered securities to manipulate or steal from the victim.
 **Business compromise**	**Business email compromise scams** involve a scammer targeting a business or individual and taking over an official account or using email spoofing to attempt to redirect payments to an illicit account controlled by the fraudster to steal from the victim.
 **Lottery/sweepstakes/ inheritance**	**Lottery/sweepstakes/inheritance scams** occur when an individual is contacted about winning a lottery or sweepstakes they never entered or to collect on an inheritance from an unknown relative.

Sources: GAO Antifraud Resource and analysis of Consumer Financial Protection Bureau, Federal Bureau of Investigation, and Federal Trade Commission information; Icons-Studio/stock.adobe.com, bsd studio/stock.adobe.com, sdecoret/stock.adobe.com, GAO (icons). | GAO-26-108842

Below are characteristics of some of the most frequently used methods by scammers to obtain funds from victims, as cited in FTC reports.

- P2P payment applications allow consumers to quickly send and receive money. Depending on the payment provider, a P2P payment can be initiated from a consumer's online bank account portal or a mobile application. According to the FTC, scammers may trick the victim into sending them money through a P2P payment application, because once the individual sends the money, it is difficult to get it back.
- Gift cards hold specific cash value that can be used for purchases. Scammers can request that individuals purchase a gift card and ask for the gift card number and PIN. Scammers deceive their victims by telling them, for example, that the gift card number is to pay the government for taxes or fines, pay for tech support, or for some other fictitious reason. The gift card number and PIN allow the scammers to access the funds that their victim has loaded into the card.
- A wire transfer is the transfer of funds from one person to another. The transfer can be domestic or international. Wire transfers can be initiated through a financial institution or a money services business.

Scams can be carried out by individuals and criminal networks operating both outside the United States and domestically. Multiple domestic law enforcement investigations have identified criminals operating from international call centers working to defraud Americans. For example, scammers in foreign-based call centers have called Americans and falsely identified themselves as federal law enforcement officers or other government officials to request that victims send money to avoid arrest or other economic consequences. The funds that criminals obtain from these scams may be linked to other illicit activities, such as human trafficking.

A 2024 DOJ study found persons aged 60 or older and persons aged 59 or younger experienced fraud at the same rate.[7] However, older adults are more likely to experience greater losses and are less likely to report scams. Agencies such as CFPB, the FBI, and FTC and Congress have initiatives designed specifically to help older adults avoid scams. Additional resources or specialized personnel are sometimes employed

[7]Department of Justice, National Institute of Justice, *Examining Financial Fraud Against Older Adults* (Mar. 20, 2024), https://www.ojp.gov/library/publications/examining-financialfraud-against-older-adults. The National Institute of Justice is the research, development and evaluation agency of the U.S. Department of Justice.

by agencies or businesses to respond to older victims, but the resolution process remains the same as for other victims.

Multiple Federal Agencies Engage in Activities to Counter Scams, but No Government-wide Strategy Currently Guides Their Efforts

Officials from the 13 federal agencies we spoke with for our April 2025 report stated that they were engaged in a range of activities related to countering scams. The agency activities cover a spectrum of roles intended to prevent, detect, and respond to scams. Each agency stated it engaged in some form of preventative activities, such as consumer education or outreach (e.g., publishing consumer alerts and articles related to fraud and scams). About half of the agencies reported engaging in information-gathering activities, such as recording or reporting on scams. Most of the agencies also reported taking some form of action to respond to or investigate scams.

Although at least 13 federal agencies engage in activities related to countering scams perpetrated against victims, each agency has its own mandate and authority, with each largely carrying out activities related to countering scams independently. However, in some instances, agencies coordinate efforts, such as by providing consumer education or by sharing consumer complaint information. For example, FTC maintains the Consumer Sentinel Network (Sentinel). Sentinel, a collaborative effort involving 46 contributors including the FBI, is a consumer-complaint reporting database made accessible to law enforcement agencies. FTC officials told us they analyze Sentinel data for consumer complaint trends and publish scam-related consumer alerts and articles on FTC's website. Some of these efforts are implemented through official bodies, such as the FTC, intended to address crimes against older adults.[8]

Officials from the 13 federal agencies we interviewed noted that they were not aware of a government-wide, or national, strategy to guide

[8]In 2022, Congress enacted the Stop Senior Scams Act, requiring the establishment of an older-adult scam prevention advisory group. In 2022, FTC established the Scams Against Older Adults Advisory Group. The advisory group focused on four main areas, and each area was led by a separate committee: (1) expanding consumer education and outreach efforts, (2) improving industry training on scam prevention, (3) identifying innovative or high-tech methods to detect and stop scams, and (4) reviewing research related to scam prevention messaging and making recommendations for future research. The advisory group's work products are available to the public at ftc.gov/olderadults. Additional information about the advisory group's work is described in the FTC's annual older adults report. Federal Trade Commission, *Protecting Older Consumers 2023-2024*.

government efforts to combat scams.[9] Our research into this topic did not identify an existing strategy that could be used government-wide to counter scams.

For our April 2025 report, FTC and Treasury shared their views with us on a single, comprehensive, government-wide strategy to counter scams. CPFB and the FBI did not offer specific views on such a strategy. According to FTC officials, no single agency has the jurisdiction and authorities to tackle the diversity of fraud and scams in the marketplace government-wide. They stated that a government-wide strategy could help overcome those jurisdictional barriers, if significant resources could be applied to tackle multifaceted and evolving scams. FTC added that any comprehensive, government-wide strategy must include a focus on criminal and civil law enforcement.

Treasury officials noted that many federal law enforcement and other agencies have overlapping mandates when it comes to fraud and scams, and a fully coordinated law enforcement strategy may in practice be difficult to coordinate and implement among agencies. Further, Treasury officials noted that to have a government-wide strategy and use it to coordinate efforts to counter scams would involve several key agencies, such as CFPB, the FBI, FTC, and Treasury.

Some industry representatives and consumer organizations have advocated for a government-wide strategy to counter scams. For example, in its November 2023 meeting, the Federal Advisory Council to the Federal Reserve Board stated in its minutes that a government-wide approach is needed to counter fraud and scams.[10] Likewise the American Bankers Association stated in a May 2024 testimony before the Senate Homeland Security and Governmental Affairs Committee's Permanent Subcommittee on Investigations that a national antiscam strategy needs

[9]A national strategy is a type of interagency coordination mechanism—typically, a document or initiative—that provides a broad framework for addressing issues that cut across federal agencies and other levels of government and sectors. We previously identified desirable characteristics for a national strategy. See GAO, *Combatting Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[10]The Federal Advisory Council, which was created by the Federal Reserve Act, is composed of 12 representatives of the banking industry selected by the Federal Reserve Banks.

to be developed.[11] According to the association, "Focusing on only one aspect or one step in the [scam] process will not stop this surge of scams. Rather, a holistic approach to address all the entities and elements of a scam has the best chance of being successful."

Other countries, such as Australia, have developed and implemented government-wide strategies and identified specific entities to counter scams, with attributable reductions in the level of scams. In this regard, Australia created a National Anti-Scam Centre within its Competition and Consumer Commission that draws on expertise across government, law enforcement, industry, and consumer groups to make Australia a harder target for scammers.[12] Together, the entities collect and share scam data and intelligence, implement scam prevention and disruption initiatives, and provide better awareness alerts and education resources to help consumers identify and avoid scams. The Australian government has reported that the National Anti-Scam Centre's efforts have led to a 13.1 percent decline in reported scam losses from 2022 to 2023.

Our prior work has shown that in some instances, it may be appropriate or beneficial for multiple agencies to be involved in the same programmatic or policy area due to the complex nature of the issue or magnitude of the federal effort.[13] However, having multiple agencies involved in the same programmatic area could create the risk of fragmentation of effort or overlap of multiple activities—especially absent

[11]The American Bankers Association is an organization that supports bankers and other members of the financial services industry with education, tools, and expert insights. The American Bankers Association also advocates for banks in legislative and regulatory issues.

[12]Australian Competition and Consumer Commission, *National Anti-Scam Centre in action: Quarterly update January to March 2024*, https://www.nasc.gov.au/system/files/NASC-Quarterly-update-Q3-2024.pdf.

[13]See GAO, *Broadband: National Strategy Needed to Guide Federal Efforts to Reduce Digital Divide*, GAO-22-104611 (Washington, D.C.: May 31, 2022); and *Broadband: A National Strategy Needed to Coordinate Fragmented, Overlapping Federal Programs*, GAO-23-106818 (Washington, D.C.: May 10, 2023).

a strategy to coordinate and manage such activities—potentially limiting their effectiveness and impact.[14]

In our April 2025 report, we recommended that the Director of the FBI lead a U.S. government effort to develop and implement a government-wide strategy to counter scams and coordinate related activities. This effort should be done in collaboration with the Director of CFPB, the Chair of FTC, the Secretary of the Treasury, and other agencies, as appropriate. As discussed below, this effort should address issues such as a common definition for scams and consumer complaint reporting. As appropriate, and consistent with desired characteristics we have identified in our prior work, a strategy should also define agency roles, responsibilities, and authorities; identify necessary resources; and identify any legislative, regulatory, or administrative changes needed to enable a comprehensive, coordinated response.

In comments to our April 2025 report, the FBI concurred with our recommendation and noted that it is fully committed to this mission and leading this effort. In October 2025, the FBI provided us with an update, stating that the development and implementation of a government-wide strategy will involve:

- **A multi-agency working group.** The FBI described the need to establish a multi-agency working group to develop an international center of excellence for the United States to mitigate the cyber-enabled fraud threat. According to the FBI, this center will allow governmental entities to share information, deconflict, and unite stakeholders, including law enforcement partners, regulatory agencies, among others.
- **Legislative updates and regulatory reform**. The FBI stated that legislative updates are needed to close legal gaps, strengthen enforcement capabilities, and ensure agencies have the necessary authorities to combat cyber-enabled fraud. In addition, regulatory reform may be needed given that cyber-enabled fraud and transnational scams continue to evolve which exposes gaps in reporting. In October 2025, the FBI informed us that it plans to work

[14]Fragmentation refers to those circumstances in which more than one federal agency (or more than one organization in an agency) is involved in the same broad area of national need, and opportunities exist to improve service. Overlap occurs when multiple agencies have similar goals, engage in similar activities or strategies to achieve them, or target similar beneficiaries. See GAO, *Fragmentation, Overlap, and Duplication: An Evaluation and Management Guide*, GAO-15-49SP (Washington, D.C.: Apr. 14, 2015).

with the Departments of Justice and the Treasury to explore areas of regulatory reform.

- **Collaboration with private sector organizations and others**. According to the FBI, improvements to fraud detection and prevention will be explored with financial institutions, tech companies, and other private sector organizations, as well as consumer advocacy organizations.
- **Additional funding**. The FBI explained that additional funding will be needed to successfully implement a government-wide strategy. This includes dedicated funding, expanded staffing, and centralized expertise, as well as acquiring advanced tools, expanding cryptocurrency tracing capabilities, and leveraging artificial intelligence and machine learning to analyze datasets to identify points of attribution.

We will continue to monitor the FBI's actions to develop and implement a government-wide strategy to counter scams.

Federal Agencies Compile Scam-Related Complaint Data, but Limitations Exist in Estimating the Extent of Scams and Related Losses

Of the eight federal agencies that receive scam-related consumer complaints, three agencies (CFPB, the FBI, and FTC) publish annual reports summarizing consumer complaint data.[15] However, the data informing these reports have limitations. For example, within the FBI, the Internet Crime Complaint Center (IC3) receives consumer complaints related to internet crime, including identity theft, data breaches, and scams.[16] The way the FBI complaint data are collected, however, limits their utility in reporting an aggregate count of the total number of complaints specifically related to scams. One such limitation is that the

[15]We identified eight federal agencies (of the 13 total agencies in our review) that receive complaints from consumers about scams. These agencies are: CFPB, the FBI, Federal Deposit Insurance Corporation, Federal Reserve, FTC, Homeland Security Investigations, Office of the Comptroller of the Currency, and Secret Service.

[16]The FBI defines internet crime as any illegal activity involving one or more components of the internet, such as websites, chat rooms, and email. Internet crime involves the use of the internet to communicate false or fraudulent representations to consumers. According to the FBI, these crimes may include, but are not limited to, advance-fee schemes, business email compromise, computer hacking, confidence/romance scams, employment/business opportunity scams, government impersonation scams, identity theft, investment scams, lottery/sweepstakes/inheritance scams, nondelivery of goods or services, and tech support scams.

IC3 does not use predefined fields that would allow consumers to indicate when a complaint is related to a scam.[17]

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. For example, FBI officials noted that FBI annual reports do not include a line item for total scam complaints received and associated dollar losses. For our April 2025 report, the FBI compiled the total at our request. According to FBI officials, in 2023, IC3 estimated that it received over 589,355 complaints related to scams, with losses of $10.55 billion. Similarly, CFPB estimated that in 2023, it received 3,210 complaints potentially regarding scams over P2P platforms. CFPB officials stated that they did not have a loss estimate for scam-related complaints because they do not require consumers to include dollar losses when filing a complaint.

The underreporting of scams also complicates calculating a government-wide estimate of scams. According to DOJ and FTC, most consumer fraud goes unreported. For example, in 2015, DOJ estimated that 15 percent of the nation's fraud victims report their crimes to law enforcement.[18] Consequently, the numbers of instances of scams and financial-loss amounts are likely understated. Similarly, a study cited by FTC reported that about 5 percent of people who experienced mass-market consumer fraud complained to a Better Business Bureau or a government agency.[19] According to FTC officials, the agency has estimated the amount of consumer fraud losses—not specific to just scams—taking into account underreporting, but officials stated more

[17]The FBI does not provide fraud or scam subcategories, such as imposter scams, that consumers can select from when making complaints. Because IC3 does not request information from consumers about the type of internet crime they encountered in a predetermined data field, it relies on consumers to include this information in an open narrative field. According to FBI officials, analysts review IC3 complaints to determine the crime type and actual dollar losses based on the information provided by the consumer.

[18]United States Attorney's Office, Western District of Washington, *Financial Fraud Crime Victims*, https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud.

[19]The Better Business Bureau accepts complaints about scams, misleading advertisements, identity theft, and other marketplace issues involving any business. Mass-market consumer fraud refers generally to any fraud scheme that uses one or more mass-communication methods, such as the internet, telephones, mail, or in-person meetings, to fraudulently solicit or transact with numerous prospective victims, or to transfer fraud proceeds to financial institutions or others connected with the scheme. Keith B. Anderson, *To Whom Do Victims of Mass-Market Consumer Fraud Complain?* (May 24, 2021), available at SSRN: https://ssrn.com/abstract=3852323, or http://dx.doi.org/10.2139/ssrn.3852323.

research was needed to accurately extrapolate a single estimate of scams based on consumer complaint data.[20]

Additionally, according to the Federal Reserve, accurate quantification of scams is often challenging because of multiple operational scam definitions and a lack of consistency in approaches for classifying different types of scams. In spring 2023, the Federal Reserve established a scams definition and classification work group. This work group consisted of payments and fraud experts from different disciplines, including federal agencies and financial institutions. The goal of the work group was to provide a more consistent foundation for scams reporting to better understand and mitigate the problem. Federal Reserve officials told us that it was important to have a consistent scam definition to help ensure that different agencies are counting the same thing, when quantifying scams.[21]

A desirable characteristic of national strategies includes defining the issue or problem that a particular strategy is intended to address. We have previously reported that the use of common definitions promotes, among other things, more effective intergovernmental operations and helps avoid duplication of effort.[22] In this regard, the definition by the Federal Reserve offers a baseline around which federal agencies and others could collaborate and arrive at a common understanding of what constitutes a scam. Alternatively, agencies could work together to develop a different agreed-upon definition.

As we explained in our April 2025 report, developing a government-wide definition of scams and improving consumer scam complaint reporting could assist agency efforts to compare data across agencies, develop an overall estimate of the total number of scams, and assess trends. Most importantly, agency efforts to improve data collection and reporting about

[20]FTC estimates that overall consumer loss from fraud, adjusting for underreporting, was as high as $158.3 billion. Federal Trade Commission, *Protecting Older Consumers 2023-2024* (Oct. 2024).

[21]In September 2023, the work group published an operational definition of scams and, in June 2024, introduced a Scam Classifier Model. The definition defines scams as the use of deception or manipulation intended to achieve financial gain. Federal Reserve Board officials told us that CFPB, the FBI, and FTC were not part of this work group and that the officials did not know what those agencies' views would be on this definition. This definition has not been adopted throughout the government.

[22]GAO, *Homeland Security: Progress Made; More Direction and Partnership Sought*, GAO-02-490T (Washington, D.C.: Mar. 12, 2002).

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. Because scammer tactics are continuously evolving with technology, having comprehensive data on scams would help agencies better understand new scams and develop ways to counter them.

Specifically, in our April 2025 report, we made 16 separate recommendations to the Director of CFPB, the Director of the FBI, and the Chair of FTC. Among these recommendations, we made the following four recommendations to each of the three agencies related to improving, in collaboration with each other, how they collect and report data on scams: (1) explore ways to harmonize data collection to better identify scams, (2) use the agency's data collection and analysis to produce and report an estimate of the number of complaints it receives and the associated financial losses resulting from scams, (3) collaborate, develop, and report on a single, government-wide estimate of the number of consumers affected by, and a dollar losses resulting from, scams, factoring in an estimate of incidents not reported and (4) develop a government-wide definition of scams. CFPB did not provide comments on our April 2025 report, while the FBI concurred with the first two recommendations listed here and did not concur with the last two. FTC neither agreed nor disagreed with the four recommendations listed here. Below are recent updates provided to us by CFPB, the FBI, and FTC on actions they have taken or plan to take in response to our recommendations.

CFPB: In an October 2025 update, CFPB did not specifically discuss actions it is taking to address the recommendations we made. However, CFPB stated that it shares our perspective that federal efforts must be as effective as possible. CFPB stated that for several reasons, such as implementation of the government-wide strategy to counter scams, it believes it is prudent to closely monitor the actions of the FBI, FTC, and other stakeholders before determining whether any further CFPB action is warranted. Further, for the recommendation to adopt the definition of scams developed by the Federal Reserve or work with the FBI, FTC, and other agencies to develop a common definition of scams and related scam types, CFPB stated that agreed-upon definitions and standards are necessary for the agency to address the GAO's recommendations in whole or in part.

FBI: In October 2025, the FBI provided an update on its actions and plans to address our recommendations.

- For the recommendation regarding data harmonization, the FBI explained that it will work with FTC and other partners to explore opportunities for alignment, such as shared scam-type classification, which would improve coordination in defining and tracking scams. The FBI added that it supports collaborative efforts to improve data consistency where alignment is feasible and mutually beneficial.
- The FBI informed us that it will explore options to more systematically aggregate and report scam-related data, including through enhancements to existing reporting platforms.
- The FBI added that it cannot address the recommendation to collaborate with other agencies to develop and report a single, government-wide estimate of the number of consumers affected by, and dollar losses resulting from, scams, factoring in an estimate of incidents not reported, as framed. However, it supports continued coordination across agencies and will do its part to contribute meaningful data and analysis to inform the government's collective fraud prevention efforts. Specifically, the FBI explained that it does not believe diverting law enforcement resources to develop independent estimates would be a wise or effective use of taxpayer funds since its focus remains on disrupting criminal networks, protecting the public, and preventing future scams. The FBI added that agencies, such as FTC, with statistical or consumer protection mandates are better positioned to lead such work.

  Our recommendation directs agencies to collaborate on developing a single government-wide estimate of scams and scam losses. We did not recommend that the FBI develop the government-wide estimate independently. As we explained in our April 2025 report, fraud estimates, including those specifically addressing scams, can demonstrate the scope of the problem, help improve oversight prioritization, and help determine the return on investment from activities to mitigate fraud.
- For the recommendation to develop a government-wide definition of scams, the FBI stated that it supports continued interagency engagement to explore opportunities for definitional alignment where appropriate. The FBI shares FTC's view that while interagency consultation is valuable, any collaborative effort to define "scams" must respect the distinct authorities, mandates, and enforcement responsibilities of each agency. The FBI noted that developing a singular, government-wide definition of scams, while conceptually beneficial, poses practical challenges, particularly given the diverse statutory frameworks under which federal agencies operate. The FBI added that it does not have the authority to compel other agencies to

adopt a unified definition and believes that any shared framework should be the product of voluntary consensus based on each agency's operational and legal context.

While we acknowledge the FBI's concerns, our recommendation calls for agencies to collaborate with each other in developing a scam definition. It is important to define terms and use definitions consistently, including using common definitions when measuring the volume and impact of scams over time. As we explained in our April 2025 report, using a common definition for this type of crime would improve the ability of agencies to compare and aggregate data across agencies, assess trends, and show progress in fraud prevention.

FTC: In November 2025, FTC provided an update on its data collection and estimate on scams efforts.

- FTC stated that harmonizing the data can be difficult but noted that it is important to provide better information to law enforcement users and better analysis to the public. The FTC explained that it will continue to review its intake mapping and will also explore ways to improve the harmonization, including the data mapping for its major contributors.
- In response to the recommendation to develop an estimate of the number of consumer reports pertaining to scams, FTC stated it will review its "fraud" and "other" topic categories in its Sentinel database to determine if there should be any adjustments to those Sentinel categories. While we appreciate FTC's effort to review its categories, this action does not address the recommendation to report an estimate of the number of complaints it receives and the associated financial losses resulting from scams. We understand that FTC already reports on fraud complaints; however, this category is broad. In our April 2025 report, we recommended FTC estimate and report the number of complaints it receives and the associated financial losses resulting from scams.
- Regarding the recommendation related to developing a government-wide estimate of scams and scam losses, FTC stated that it already makes efforts to report its fraud-related data and estimates of consumer impact, which include reports from many other government agencies, such as the FBI. According to FTC, its 2023 report to Congress, Protecting Older Consumers, estimated $158.3 billion in consumer fraud losses in 2023, with an estimated $61.5 billion lost by

older adults.[23] However, this estimate is not a single, government-wide estimate of losses resulting from scams. As we stated in our April 2025 report, we understand that each agency has its own mandate and authority. We continue to believe, however, that a single, government-wide measure and a common definition of scams will best support a multiagency approach and response to scams.

- Regarding the development of a common definition of scams, FTC expressed concerns about the uniform adoption of the Federal Reserve's definition of "scams." FTC officials stated that they have used the terms "scam" and "fraud" interchangeably for many decades, and they have established methods for tracking consumer report data. Further, the FTC explained that the Federal Reserve's definition of scam does not align with its statutory responsibilities related to prohibiting a wide range of conduct. FTC agreed that additional collaboration with CFPB, the FBI, and other agencies is needed to fight scams and fraud.

  As the Federal Reserve has made clear, accurate quantification of scams is often challenging because of multiple operational scam definitions and a lack of consistency in approaches for classifying different types of scams. Federal Reserve officials told us that it was important to have a consistent scam definition to help ensure that different agencies are counting the same thing, when quantifying scams. Further, a common definition is necessary for the development of a government-wide strategy. Our recommendation gives FTC an option to adopt the definition of scams developed by the Federal Reserve or work with CFPB and the FBI and other affected agencies to develop a common definition of scams and related types. While we understand there may be limitations with agencies' authority and the Federal Reserve scam definition, we continue to believe that the agencies should work together to adopt a definition of scams.

While the three agencies 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. Given the scope, scale, and nature of scams targeting consumers and the extent of financial and other harm they inflict, swift action by these agencies is needed to implement our recommendations. As discussed above, some agencies noted in our April 2025 report that they did not agree with some of our recommendations—such as establishing a common definition of scams

[23]FTC, *Protecting Older Consumers 2023–2024* (Oct. 18, 2024) https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf.

and estimating the extent of scams. While we acknowledge the challenges involved in such undertakings, we continue to believe our recommendations are warranted and should be implemented expeditiously. Accordingly, we will continue to monitor the three agencies' efforts to implement our recommendations.

Chairman Scott, Ranking Member Gillibrand, and Members of the Committee, this concludes my prepared statement. I look forward to your questions.

GAO Contacts and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Seto J. Bagdoyan, Director, Forensic Audits and Investigative Service at BagdoyanS@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are David Bruno (Assistant Director), Samantha Sloate (Analyst in Charge), Colin Fallon, Brenda Mittelbuscher, Gloria Proa, Joseph Rini, Daniel Silva, and Rachel Steiner-Dillon.

Questions for the Record

U.S. SENATE SPECIAL COMMITTEE ON AGING

"MADE IN CHINA, PAID BY SENIORS: STOPPING THE SURGE OF INTERNATIONAL SCAMS"

JANUARY 14, 2026

QUESTIONS FOR THE RECORD

Kathy Stokes

Senator Raphael Warnock

Question:

According to the Federal Trade Commission, financial fraud was more prevalent in Georgia than in any other state in 2023, with 437 incidents per 100,000 individuals. In 2023, Georgians aged 60 and older reported losses of over $92 million to the Federal Bureau of Information's Internet Crime Complaint Center. To address this issue, I co-introduced S. 2019, the Task Force for Recognizing and Averting Payment Scams Act, which would establish a multi-agency task force to examine fraud trends and lead prevention efforts. Last Congress, I also reintroduced the Empowering States to Protect Seniors from Bad Actors Act, which would create a new grant program to protect senior investors.

How would multi-agency coordination and federal grant programs focused on investigating fraud protect Georgia seniors from financial scams?

Response:

Multi-agency coordination is critical because today's fraud schemes rarely fall neatly within the jurisdiction of a single agency. Scams targeting older adults often involve online platforms, financial institutions, telecommunications providers, and, in many cases, actors operating across state or national borders. A coordinated task force, such as the one that S. 2019, the TRAPS Act, calls for, would bring together the expertise and authorities of agencies such as the FTC, DOJ, FBI, and state attorneys general to share data in real time, identify emerging scam trends, and respond more quickly when patterns of fraud begin to appear. This kind of coordination helps move the response from being reactive-after money is lost-to preventative, stopping scams before they spread widely in communities like those across Georgia.

Federal grant programs, such as contemplated in the 118th Congress' Empowering States to Protect Seniors from Bad Actors Act or 119th Congress' S. 2544, the GUARD Act, or H.R. 6426, the Stop Scams Against Seniors Act, play a critical role by ensuring that states have the capacity to act on that shared intelligence. Many state and local agencies, including those in Georgia, are on the front lines of protecting seniors but lack the dedicated resources to investigate complex financial fraud cases or to conduct sustained outreach and education efforts. Grant funding can support specialized task forces, investigators, partnerships with financial institutions to flag suspicious transactions, and community-based education programs that help older adults recognize red flags before they become victims.

Thank you for your leadership on this issue. We are experiencing a fraud epidemic and it is critical that we work together to prevent seniors from being exploited in the first place, as well as provide the necessary support when fraud does happen.

U.S. SENATE SPECIAL COMMITTEE ON AGING

"MADE IN CHINA, PAID BY SENIORS: STOPPING THE SURGE OF INTERNATIONAL SCAMS"

JANUARY 14, 2026

QUESTIONS FOR THE RECORD

Seto Bagdoyan

Senator Raphael Warnock

Question:

A recent report from the Government Accountability Office identified the Federal Trade Commission (FTC), Consumer Financial Protection Bureau (CFPB), and the Federal Bureau of Investigation as the federal agencies best positioned to lead a government-wide strategy on anti-scam efforts. As you know, President Trump fired the two Democratic Party members of the five-member FTC in March 2025, and the administration has attempted to eliminate the CFPB.

How have these disruptions to the federal workforce affected the capacity of these agencies to combat scams targeting older adults?

Response:

In April 2025, GAO issued a report (GAO-25-107088) identifying federal efforts to prevent, detect, and respond to scams. We made 16 separate recommendations to the Consumer Financial Protection Bureau (CFPB), Federal Trade Commission (FTC), and the Federal Bureau of Investigation (FBI) to better prevent, detect, and respond to scams. Specifically, we recommended that the FBI lead a U.S. government effort to develop and implement a governmentwide strategy to counter scams and coordinate related activities. We also made recommendations to CFPB, FTC, and the FBI related to improving, in collaboration with each other, how they collect and report data on scams.

Pursuant to Standards for Internal Control in the Federal Government, agency management is responsible for recruiting, developing, and retaining competent personnel to achieve the agency's objectives. A lack of competent personnel can result in skill gaps, which occur when agencies have an insufficient number of individuals or individuals without the appropriate skills or abilities to successfully perform their work. GAO's 2025 High Risk List notes that skills gaps within agencies impede agencies from cost effectively serving the public and achieving desired results. GAO has also previously issued work on assessing government reorganization efforts (GAO-18-427). As the report notes, strategic workforce planning should occur before any staffing changes to avoid creating skill gaps or other adverse effects that could impair agencies' ability to carry out their missions.

GAO has not yet evaluated the impact, if any, of recent administrative and personnel actions at CFPB, FTC, and the FBI. On July 7, 2025, Senators Kirsten Gillibrand and Elizabeth Warren-later joined by Senator Maggie Hassan-requested GAO examine the impact of recent administrative and personnel actions on the ability of the federal government to address fraud and scams and implement the recommendations from our April 2025 report. GAO recently staffed this engagement and will commence work very soon.

Statements for the Record

NAELA
National Academy of Elder Law Attorneys

1577 Spring Hill Road, Suite 310 // Vienna, Virginia 22182
naela@naela.org // 703-942-5711 // www.NAELA.org

Statement
of the
National Academy of Elder Law Attorneys
for the
Special Committee on Aging
of the
United States Senate
"Made in China, Paid by Seniors: Stopping the Surge of International Scams"
January 14, 2026

On behalf of our more than 4,000 members who are attorneys representing older Americans and individuals with disabilities, the National Academy of Elder Law Attorneys (NAELA) writes to express our strong support for legislation to combat the growing number and increasingly sophisticated nature of scams targeting older adults. NAELA is the leading professional association dedicated to improving the quality of legal services for older Americans and individuals with disabilities. With 31 active state chapters, NAELA provides elder and special needs law attorneys with education, advocacy, community, and the resources they need to better serve their clients.

Scams have a devastating financial impact on older Americans. In December, the Federal Trade Commission reported that older Americans lost more than $2.4 billion in scams in 2024, up from $600 million in 2020, although it estimates that number may be as high as $81 billion due to unreported instances of scams. Single older adults are particularly at risk, given their more limited support from family and the community. As the witnesses discussed at the hearing, there are a wide variety of scams targeting older Americans, including romance, tech support, investment, and impersonation scams, with some scammers grooming individuals over months and convincing these vulnerable adults to loan them money from their retirement accounts. Faced with the loss of their retirement nest egg, these well-meaning individuals are then hit with the double whammy of paying taxes on money they no longer have, further harming them financially.

As elder law attorneys, NAELA's members help clients take steps to avoid or minimize the effects of scammers' actions, such as creating a durable power of attorney; instituting protective arrangements, guardianships, and conservatorships through the courts; designating a "trusted contact" with brokerage or other financial accounts; or placing a freeze on Social Security numbers with credit bureaus. However, such preventative action is not always possible before a scam takes place. That is why NAELA is proud to support

two pieces of bipartisan legislation to help combat scams, both of which are sponsored by Chairman Scott, Ranking Member Gillibrand, and other committee members.

The Guarding Unprotected Aging Retirees from Deception (GUARD) Act (S. 2544 and its House companion, H.R. 2978) would protect seniors from financial frauds and scams by increasing resources and personnel to use blockchain technology to investigate financial fraud; it would also encourage greater cooperation between federal and local law enforcement. Additionally, the National Strategy for Combating Scams Act (S. 3355 and its House companion, H.R. 6425) would establish a federal working group to coordinate anti-scam efforts, and improve coordination at the federal, state, and local levels. Both bills are necessary to help the government stop scams *before* they have the potential to wreak havoc on individuals' lives, particularly those of some of our most vulnerable citizens.

We appreciate the attention the committee has brought to this important issue by holding this hearing. Taking action to better target and address scams affecting older adults should be a no-brainer. Otherwise, scams, particularly those using AI, will only become harder to spot and more effective in taking money from their victims, devastating people as they try to prepare for and enjoy their retirement. We encourage all Senators on the committee to support this legislation, and we urge Congress to pass these bills as soon as possible.

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

United States Senate
Special Committee on Aging

Statement for the Record

Made in China, Paid by Seniors: Stopping the Surge of International Scams

Michelle L. Anderson
Assistant Inspector General for Audit
as First Assistant

Social Security Administration
Office of the Inspector General

January 14, 2026

Chairman Scott, Ranking Member Gillibrand, and members of the Committee. I want to thank the Special Committee on Aging for holding today's hearing entitled "Made in China, Paid by Seniors: Stopping the Surge of International Scams."

The Social Security Administration (SSA) Office of the Inspector General (OIG) is a key federal player in the fight against government imposter scams. Many of these scams originate from overseas and reach our American shores, stealing significant amounts of money from Americans.

In 2024, according to the Federal Trade Commission (FTC) consumers reported losing $12.5 billion to scams, including government imposter scams. FTC estimates that, when adjusted for underreporting, Americans may have actually lost a staggering $158 billion to scammers.

Scams are known to be linked to transnational criminal organizations. National security and economic stability are at serious risk. International scammers are viciously attacking Americans, and we are all vulnerable.

Hard-earned money from the American public leaves the United States and is being utilized to fuel their criminal enterprises, which according to reports from the FTC and the Federal Bureau of Investigations (FBI), may often involve organized crimes such as drug and human trafficking. Moreover, scammers will also draw Americans into their crimes to facilitate the transfer and movement of stolen funds.

Hearings, such as one today, provide an important reminder to every American to be vigilant and to protect their money and personal information from scammers. Individual awareness and skepticism when contacted by telephone, text, email, social media, and even U.S. mail ploys, is the first line of defense in identifying and preventing a scam.

Scammers exploit human emotion; fear, intimidation, trust, urgency, loneliness, sympathy, and even hope can be used to manipulate people into complying with demands. These criminals are relentless in their efforts to gain access to Americans' money or personal information. Even when scammers fail to obtain direct payment from their victims, they use Americans' identities and monetize them for criminal activity.

Social Security scams are widespread across the country and reach people of all ages. However, seniors are disproportionally affected. As noted in SSA OIG's most recent *Scam Update to Congress*, individuals of all ages report scams, but individuals aged 70 and over report significantly higher financial losses to scams.

The goal is to prevent Americans' personal information and hard-earned money from leaving the United States, because retrieving this information or lost financial assets from malign actors outside the United States is nearly impossible.

The scams can be complex: a scammer contacts an American and tells them they must pay a fine or provide information to avoid arrest or other legal action, resolve a Social Security number problem, or increase a benefit. They demand money using difficult to trace forms of payment, such as cash, retail gift cards, pre-paid debit cards, gold bars, or cryptocurrency. Scammers often apply immense pressure and quickly escalate threats to frighten victims into complying. Scammers have emailed fake letters that appear to come from Social Security, utilizing official looking letterhead or the publicly available names of actual SSA and SSA OIG employees, to convince potential victims of their legitimacy.

While SSA OIG has seen a precipitous decline in reports of SSA-related imposter scams from 2020 to the present, SSA-related scams remain a top-reported government imposter scam. In fact, according to FTC data, SSA remains the top federal agency used in schemes by criminals to defraud Americans.

SSA OIG has taken a multi-disciplinary approach to combatting SSA-related government imposter scams. For five years, SSA OIG has investigated emerging major fraud schemes against SSA programs and operations, including government imposter scams. Investigating large-scale organized fraud often requires a multi-disciplinary effort with enhanced legal and analytical capabilities, and coordination with multiple law enforcement agencies around the country. OIG works zealously to develop leads, disrupt the scams, and provide evidence for criminal prosecutors. For example, our work with federal and state partners has led to the prosecution and sentencing of multiple individuals involved in telephone imposter scams originating from overseas call centers.

SSA OIG agents and attorneys also notify domestic gateway telecommunications providers (who serve as intermediaries between foreign providers and downstream American telecom carriers and pass-through millions of calls daily) of their potential civil liability under a consumer protection law within the *Social Security Act*.[1] In doing so, SSA OIG attorneys educate these domestic gateway providers on the applicability of this statutory provision, encourages proactive techniques to identify and block transmission of scam calls both domestically and internationally, and, where appropriate impose fines.

Artificial Intelligence (AI) is rapidly becoming a primary driver of emerging technologies and is impacting society in ways the public and private sectors are just beginning to understand. China and other nations are in a race with the United States to develop and implement AI. While criminals have used AI to increase the volume and speed of their criminal activities, AI has also become an important technology in fraud detection. It is possible to thwart fraud attempts by using large data sets to continuously train fraud detection algorithms to predict and recognize anomalous patterns indicative of fraud in the private and public sectors.

AI will continue to be a powerful tool to support the Federal Government's ability to detect and prevent the fraudulent disbursement of taxpayers' dollars. AI is also a formidable tool for international criminals to engage in widespread and repeated scams at a low cost. Criminals use AI to make scams easier and faster to execute, the deceptions more credible and realistic, and ultimately, the scam more profitable.

SSA OIG is concerned about how scammers will continue to utilize AI to increase the frequency and sophistication of scams against Americans. SSA OIG's goal is to be at the forefront by leveraging AI to detect fraud, improve decision making, and learn rapidly how AI can be used in new and emerging ways to commit malicious behavior.

---

[1] Section 1140 of the *Social Security Act* (42 U.S.C. § 1320b-10), as amended, protects the public from advertisements, solicitations, and other communications (including websites and scam telephone calls) that may convey the false impression SSA approved, endorsed, or authorized the communication. It also prohibits the reproduction and sale of SSA publications and forms without authorization and places restrictions on charging for services SSA provides to the public for free.

SSA OIG established a Task Force to study AI and related technology. From this effort, SSA OIG is working to determine the tools, processes, and staffing needed to detect, investigate, and deter AI-related fraud and to leverage AI in fighting fraud. SSA OIG will continue to work with longtime federal law enforcement partners to stay current in the detection, investigation, and deterrence of AI-related fraud. The goal of the SSA OIG AI Task Force, through collaboration with the agency, is to also work to ensure SSA unwraps the potential transformational impact of AI to benefit the American public in a way that balances enhanced customer service and limits the risk of fraud.

SSA OIG also collaborates with SSA through the National Anti-Fraud Committee (NAFC), a partnership of senior leaders dedicated to combating fraud, waste, and abuse in SSA programs. Meeting quarterly to share information and develop actionable strategies, the NAFC also hosts an annual multi-day summit for SSA and SSA OIG subject matter experts, fostering collaboration, addressing challenges, and identifying vulnerabilities.

NAFC has been the breeding ground of ideas for the need to use AI to fight fraud, waste, and abuse and the need to fight AI-related fraud. Following each summit, SSA OIG and SSA mutually agree upon action items to enhance the efficiency and effectiveness of agency operations. The NAFC summits have been critical in leading to significant improvement in fighting fraud waste, and abuse and promoting the efficiency and effectiveness of SSA's programs and operations.

In fact, following the Fiscal Year 2023 NAFC summit, SSA and SSA OIG agreed to establish the NAFC AI Subcommittee, which consists of the SSA OIG AI Task Force members and SSA's AI Core Team, including its Chief AI Officer. The NAFC AI Subcommittee meets quarterly and discusses SSA's compliance with M-25-21, its AI Strategy and Compliance Plain, its current inventory of AI-use cases, and AI-use cases in development. It also explores risk assessments and identifies vulnerabilities in SSA's AI-use cases, contributing to enhanced oversight through improved fraud detection and mitigation strategies. Additionally, the Task Force has assisted SSA in spotlighting and addressing AI threats, mostly identified through NAFC-related activities.

Mr. Chairman, scams against Americans erode the public's trust in SSA, and in the Federal Government overall. SSA OIG will continue to engage with agencies like the FTC and Federal Communications Commission (FCC), who have proven capable partners in our fight against government imposter fraud. SSA OIG meets regularly and collaborates with SSA to understand how the agency plans to use AI in its operations, and will review any applicable risk assessments, vulnerabilities, and/or efficiencies gained utilizing AI in SSA programs. Additionally, with our oversight tools, we plan to assist SSA to address AI threats to the agency and to Social Security numberholders.

SSA OIG is committed to educating the public about scams by individuals pretending to be from SSA or SSA OIG to empower the public to identify and prevent the scams themselves. SSA OIG educates the public through a multidisciplinary public awareness campaign. Along with public and private partners, the media, the United States Congress, and agencies across the Federal Government, SSA OIG works tirelessly to try to reach every American to reduce the number of people who lose money and personal information to these pervasive and insidious scams.

I, especially, want to take a moment to recognize Chairman Scott and Ranking Member Gillibrand and members of the Committee who have supported SSA OIG's annual National Slam the Scam Day. In 2025, Chairman Scott and Senator Kelly took the lead to introduce and

pass by unanimous consent the bipartisan resolution S.J. Res 118 during National Consumer Protection Week.

National Slam that Scam Day is the centerpiece of SSA OIG's year-round public-awareness campaign. National Slam the Scam Day, as this hearing is doing today, educates the public about the tactics scammers use and encourages the public to "slam" scammers. Providing awareness and tips for spotting scams is a major thrust of the National Slam the Scam Day public awareness campaign.

Education and outreach continue to be a powerful tool, empowering consumers to protect themselves and their communities from scams. SSA OIG will continue to urge Americans to disconnect from interactions with scammers, whether on the telephone, via text, social media, or email. It is our goal to keep Americans well informed of the tactics scammers use, new and emerging scam trends, and available resources.

SSA and SSA OIG's joint website www.ssa.gov/scam shares resources, tips, and alerts and allows individuals to report Social Security-related scams. Americans can help SSA OIG by continuing to report scams, providing valuable data for investigative leads and targeted outreach. SSA OIG will continue to urge each American to be cautious of any contact supposedly from a government agency telling you about a problem you do not recognize.

Real government officials will NEVER:

- Threaten arrest or legal action against you unless you immediately send money;
- Promise to increase your benefits or resolve a problem if you pay a fee or move your money into a protected account;
- Require payment with gift cards, prepaid debit cards, wire transfer, Internet currency, gold bars, or by mailing cash; or
- Try to gain your trust by providing fake "documentation," false "evidence," or the name of a real government official.

Unfortunately, the scams and the scammers continue to evolve, and we at SSA OIG always expect they will soon move on to new tactics and techniques. Further, we are constantly monitoring what transnational criminal organizations are doing to infiltrate and commit scams against Americans.

These scammers have robbed too many individuals of their hard-earned savings, and the Federal Government must continue to leverage resources across agencies and use innovative approaches to stop the scams and protect Americans. At some point soon, most Americans will have experienced, or know someone who has experienced, losing money or personal information to a scam.

Thank you for holding this hearing today to discuss ways to protect Americans from these scams. Raising public awareness, without question, is one of the most effective ways to combat scams. By educating all Americans, we can help them identify, prevent, and report scams. Thank you again for the opportunity to submit the statement for the record.

Statement for the Record

United States Senate Special Committee on Aging

Hearing:
Made in China, Paid by Seniors: Stopping the Surge of International Scams

January 14, 2026
Washington, DC

Ken Westbrook
Founder and CEO, Stop Scams Alliance
www.StopScamsAlliance.org

Dear Senator Scott, Ranking Member Gillibrand, and Members of the Committee:

SUMMARY
Stop Scams Alliance is a 501(c)(3) nonprofit whose mission is to significantly reduce scams in the United States through a comprehensive, systemic approach involving public-private partnership and cross-sector cooperation from technology, telecom, financial institutions, consumer advocacy groups, and government. The focus is to stop scams at the source, before they reach the consumer in the first place.

We respectfully submit this Statement for the Record because our nation faces a dire and fast-growing threat to our national security, our citizens, and our financial institutions. The United States must move rapidly to increase our defenses against transnational criminals who are using increasingly sophisticated cyber-based techniques to scam Americans at unprecedented scale.

Our initial focus should be to:

1) Create the proper organization and authorities to defend the nation from attack by foreign cybercriminals. Congress should declare that fighting cyber-enabled financial crime is a national priority, appoint a leader in the Executive Branch to create and implement a national anti-scam strategy, and provide sufficient resources to combat the transnational criminals.

2) Centralize the collection and fusion of data to provide a better picture of the threat and to accelerate our ability to respond.

3) Measure the problem and the nature of the threat. Good public policy requires good data.

Additional proposals for combating the surge in cyber-enabled financial crime include:

- Improve authentication of the main communications pathways used by scammers, including fake advertising and spoofed phone calls and text messages. Improved authentication will help address impersonation scams, which the FTC says are consistently among the top frauds.

- Create a national capability to quickly take down malicious websites created by criminals, especially fraudulent investment websites. Investment scams are the costliest cybercrime tracked by the FBI.

- Boost law enforcement resources and intelligence priorities, including funding for investigators and improved scam training for law enforcement personnel.

- Mount a focused government-industry effort to combat the "Tech Support Scam," the number one scam afflicting our senior population measured by the number of victims.

- Limit payments to crypto ATMs because of the disproportionate harm they are causing to older Americans.

Who are the perpetrators?

Our response to the scam crisis should start by recognizing the nature and origin of the threat. Today's scams are not isolated acts by individuals. They are mainly transnational, industrialized operations**,** driven principally by organized crime groups in China, Southeast Asia, South Asia, Mexico, and West Africa**.** The United States faces a cyber-enabled attack by Transnational Organized Criminals who are waging an economic war on our country, stealing hundreds of billions each year. Older Americans are sitting ducks.

Senator Grassley was correct to open a Judiciary Committee hearing in June 2025 by saying "Transnational Organized Crime groups are targeting all of us with industrial-scale fraud." Grassley mentioned criminal groups in Southeast Asia, Nigeria, and India and he said: "Let me be absolutely clear: this is a national security crisis hiding in plain sight." He also said: "This isn't just a call to protect the elderly. It's a call to defend our country's integrity, its financial security and its moral obligation to protect the innocent."

According to FBI, UN, and Interpol reports, the perpetrators of scams include ethnic Chinese crime syndicates located in **Southeast Asia**—Burma (Myanmar), Cambodia, Laos, and other countries. In the last few years, the criminals have expanded beyond Southeast Asia. The Center for Strategic and International Studies reports that "Though media coverage often focuses on Southeast Asia, scam centers have also been discovered as far away as Ghana, Peru, the UAE, and Mexico. Many, though not all, of these centers can trace their ownership back to Chinese-speaking criminal groups."

Who is behind the pesky "toll road" scam that we've all received via text message? Chinese cybercriminals. The Wall Street Journal wrote in October 2025: "Criminal organizations operating out of China, which investigators blame for the toll and postage messages, have used them to make more than $1 billion over the last three years, according to the Department of Homeland Security."

Cybercriminals who focus on consumer scams are also located in:

- **South Asia**. Call center scams primarily emanate from South Asia, mainly India, according to the FBI. Such call center scams overwhelmingly target older Americans.

- **Mexico**. The Treasury Department issued a press release in August 2025 that says Mexican drug cartels use timeshare fraud to supplement their drug trafficking proceeds. These scams take place via phone and email and often target older Americans.

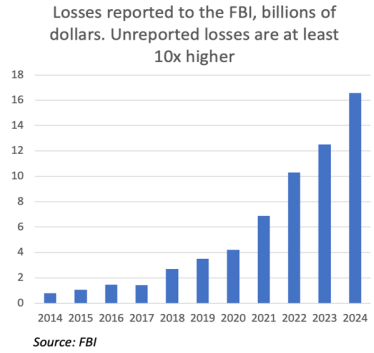
- **West Africa**. According to Interpol, the Nigerian Black Axe criminal organization and other West-African organized crime groups are responsible for much of the world's cyber-enabled financial fraud. Criminals engaged in the growing wave of "sextortion" scams that target teens are primarily in West African countries such as Nigeria and Ivory Coast or Southeast Asian countries such as the Philippines, according to the FBI.

The scale of the threat

A recent Federal Trade Commission report estimates that *total* U.S. fraud losses (reported and unreported) are approximately **$196 billion** annually. Losses at this level would exceed the

annual revenue of such corporations as General Motors, Bank of America, or Meta. It would also be about double the annual budget of the Department of Homeland Security.

The growth rate of scams is skyrocketing. According to FBI data, losses reported to the FBI have quadrupled since 2020; reported losses ballooned 33 percent between 2023 and 2024 alone.



According to Gallup, financial scams are now among the most common crimes affecting US adults. For the last three years, Gallup surveys have shown that the two top crime-related concerns in the country are identity theft and scams. Nearly all Americans say online scams and attacks are a problem for people in the United States, including about eight-in-ten who say they are a *major* problem, according to Pew Research.

Small businesses, too, report that fraud losses have surged since 2020. According to the latest data from Experian, financial fraud against small businesses has increased by 70% since 2020, costing billions annually.

U.S. law enforcement is overwhelmed by the tsunami of fraud. A Secret Service official testified in 2024 that "transnational fraud threats far exceed the current capacity of U.S. law enforcement to sufficiently deter." A Deputy District Attorney from the San Diego District Attorney's Office testified in a 2024 Senate Aging Committee hearing that "we are only able to work on one tenth of one percent of the cases we see."

The result: hundreds of billions of dollars are flowing from the United States into the coffers of foreign criminals each year. The proceeds are used to fuel more organized crime, including human trafficking, drug trafficking, and narco-terrorism. Criminals are increasingly using artificial intelligence to make their scams more realistic, which will turbocharge fraud.

Scams must be treated as a new national security threat

Scams and fraud perpetrated by foreign crime gangs are a threat to our nation's security.

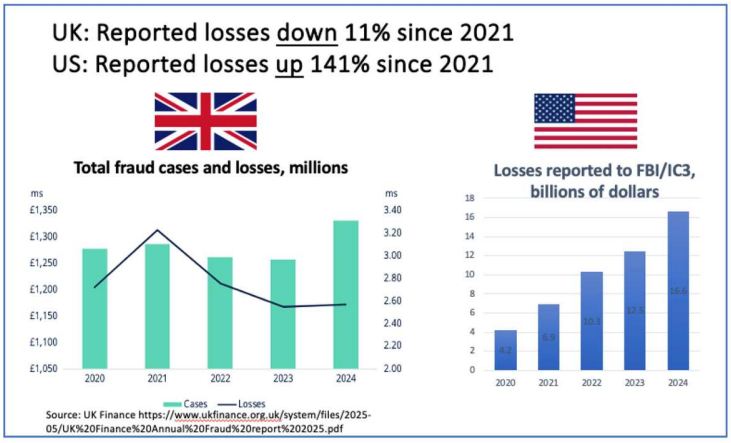
In February 2025, Google issued a report entitled: "Cybercrime: A Multifaceted National Security Threat." The report urged policymakers to elevate cybercrime as a national security priority. Microsoft also has called the threat environment "complex, challenging, and increasingly dangerous." Microsoft called for government action, saying: "We have to find a way to stem the tide of this malicious cyber activity."

In September 2025, 46 companies—including Amazon, Google, Meta, Microsoft, JPMorganChase, and Target—signed a letter to Congressional leadership that said:

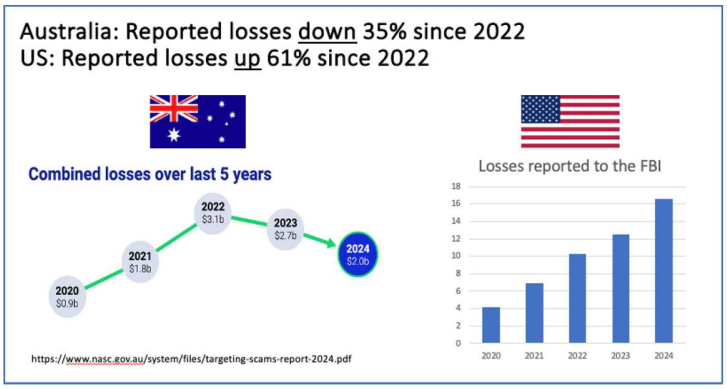
> **…** fraud and scams have become a fast-evolving **national security threat**. Proceeds from these illegal activities are a critical funding source for transnational criminal organizations—fueling drug cartels, human trafficking, and terrorism. These same networks are also targeting a broad swath of U.S. companies—including the financial services, telecommunications, and technology industries—in an effort to erode public trust and destabilize the economy.

It is possible to bend the curve

Government actions in the UK and Australia are showing signs of progress in the battle against scams. Both countries report declines in fraud losses in recent years. The below chart shows that in the UK, reports of fraud have increased slightly, but reported fraud losses are relatively flat since 2021, according to the British trade organization UK Finance. This contrasts with the significant increasing losses reported by Americans to the FBI over the same period.



Australia reports a sustained decline in reported fraud losses since a peak in 2022. The below graphic compares the fraud losses reported to the Australian government over the last five years with those reported in the U.S. to the FBI over the same period.



Why are Australia and the UK making progress in the fight against scams? Both countries have:

- A national coordinator for fraud policy to spearhead a comprehensive national strategy, including goals and metrics (the Home Secretary in the UK, the Minister for Financial Services and Assistant Treasurer in Australia).
- Mechanisms for enhanced public-private partnership.
- Annual government surveys to measure the extent of fraud.
- Centralized reporting mechanisms and information fusion hubs, which enable a fuller view of scam threats and a faster ability to respond.
- Authentication measures to reduce spoofed phone calls and text messages, fake online advertising, and fake investment websites, plus a national capability to quickly take down fraudulent investment websites.
- Increased law enforcement resources.
- Nationwide education campaigns.
- Improved authentication of financial transactions and accounts.
- Modest new government investment in anti-scam efforts. Each country has found that the investment of a few hundred million dollars can significantly reduce fraud losses.

Recommendations for Congressional Consideration

It's time to make the fight against foreign organized crime gangs a national priority in the United States. Our initial focus should be to:

- Create the proper organization and authorities to defend the nation from attacks by foreign cybercriminals.
- Centralize the collection and fusion of data to provide a better picture of the threat and to accelerate our ability to respond.
- Measure the problem and the nature of the threat. Good public policy requires good data.

We should:

1. Create a national strategy to combat consumer fraud
Congress should declare that fighting foreign cyber scams is a national priority, appoint a leader in the Executive Branch to create and implement a national anti-scam strategy, and provide sufficient resources for the battle with transnational cybercriminals. The strategy should clarify authorities about who is in charge in the U.S. Government, and create a national *whole-of-society effort*, including mechanisms for enhanced public-private partnership involving the technology, telecommunications, and financial sectors. The strategy should set goals and measure progress.

A. Create a White House-level coordinator. To defend the nation from a foreign cyber-enabled attack, a single point of leadership is needed to coordinate fraud and scam policy.

We request that the Committee consider the merits of a bipartisan bill introduced in December 2025 by members of the House Stop Scams Caucus. The *National Scam Prevention Coordination Act* (H.R. 6681) would establish an office in the White House to oversee and coordinate the implementation of a national strategy for fraud and scam prevention. The duties of the National Fraud and Scam Prevention office would include:

- Serving as the principal advisor to the President on scam and fraud prevention policy and strategy.
- Coordinating the implementation of national fraud and scam prevention policy and strategy with federal agencies.
- Annually reporting to the President and Congress on the effectiveness of national fraud and scam prevention policy and the status of implementation.

When confronted with complex global challenges in the past, the United States has responded by appointing a White House-level leader to formulate a focused, whole-of-government response.

- In the 1980s, **The Anti-Drug Abuse Act of 1988** created the Office of National Drug Control Policy (ONDCP) within the White House, establishing a single point of leadership to coordinate federal drug control efforts and develop a unified national strategy.

- Congress used a similar playbook in 2021 to address the complex nature of cyber threats. It created the Office of the National Cyber Director (ONCD), which provides centralized leadership on U.S. cybersecurity policy, coordinating efforts across federal agencies to improve the nation's cyber posture.

B. Create a national-level anti-scam strategy, including a *"public-private partnership and a "multisectoral, whole-of-society effort."* The Congress sought to do that in the 2024 Financial Services and General Government Appropriations Bill, which directed the Treasury Department to "*facilitate a public-private partnership and a "multisectoral, whole-of-society effort."* The Bill directed the Treasury Department to issue a report by March 2025, but no report was issued.

At least 13 bills were introduced into Congress in 2025 that would create a task force to create a national strategy. In our view, such a task force should include the following characteristics:

- Led by a White House-level official.
- Include representation from the entire scam ecosystem, including big tech and social media platforms, online advertising, telecommunications providers, and the financial sector.
- Include cyber expertise. Since most scams are cyber-enabled, the task force should include representatives from government agencies concerned with cyber threats, such as the Department of Homeland Security (DHS).
- Include sufficient personnel and budget for the project to succeed.

Congress could also authorize a **Federal Advisory Committee** (FAC) to create a whole-of-government strategy, drawing on expertise from both public and private sector experts. FACs offer benefits over government task forces, primarily due to their structured, ongoing nature and emphasis on external expertise. They also are designed to enable deeper public engagement and transparency compared to internal government task forces.

C. Improve Legislative Branch coordination. Given the severity and complexity of the fraud threat, Congress should consider creating a coordinating body similar to the Senate Caucus on International Narcotics Control. A "**Senate Caucus on Fraud and Scam Prevention**" would help coordinate a holistic response to a complex problem that involves many Congressional committees.

Building on the Stop Scams Caucus in the House of Representatives, the creation of a bipartisan **bicameral caucus** would help build cross-chamber coalitions, facilitate information sharing, and raise issue awareness, as seen in other bicameral caucuses that have been successful in the past.

D. Create a formal mechanism for enhanced public-private partnership. Several international models exist.

- The British government is working closely with the private sector, including tech, telecoms, and financial institutions. In an "Online Fraud Charter" announced in November 2023, large tech companies volunteered to take nine major steps to reduce fraud on their platforms.

- Australia created a National Anti-Scam Centre (NASC) in 2023 that brings together government agencies, law enforcement, and industry participants from the finance, telecommunications, and digital platform sectors to fight scams. Also in Australia, nine major technology companies (including Apple, Discord, Google, Meta, Snap, TikTok, Twitch, X and Yahoo) signed "*The Australian Online Scams Code*" in 2024, which serves as a blueprint for best practice for how to combat scams online.

2. Centralize reporting and enhance information sharing and data fusion

Centralization and information sharing across government and the private sector would help us identify the threats and respond. At least a dozen nations around the world now have national anti-scam centers because they have proven to be very effective. Why not the United States?

A. Create a central reporting mechanism so victims can report easily and quickly. Congress should authorize the creation of a centralized method for reporting scams. Americans should be able to easily report either an attempted scam or a scam that has succeeded. An easy, standardized way for people to report being scammed would:

- Improve our understanding of the threat picture.
- Enable quicker reaction.
- Be less costly than our existing system, which is redundant and inefficient.

The current system is duplicative, confusing, and ineffective. The FTC estimates that only between 2 and 6.7 percent of scam victims report to the FTC. In a recent poll conducted by the Global Anti-Scam Alliance, about 5 percent of Americans said they don't report because of shame, but the vast majority of people say they don't report because they don't know how to, or it's too complicated, or they don't think reporting would do any good.

The current reporting system looks like a maze to victims, with many potential places to report.

B. Improve cross-industry information sharing. Congress should create a way to encourage financial institutions to report fraud to a central repository easily accessible by law-enforcement authorities and other financial institutions. Because studies show that victims are more likely to report fraud to their bank than to the federal government, this approach would provide much more timely and complete information than our current process of relying mainly on reports from victims who report to the FBI, FTC, Treasury/FINCEN, or other agencies. The repository should include details such as IP addresses, device information, sender/receiver information, and amounts.

- This type of reporting would capture much more fraud than the current Suspicious Activity Report (SAR) system, which is limited to fraud amounts over $5,000 in most cases.

- Also, SAR access by state and local law enforcement is limited; state and local officials generally must request access through appropriate channels and don't have direct database access. A shareable repository would provide near-real-time insights on trends, which would allow us to move more quickly to counter emerging threats.

A Federal Reserve-backed working group recommended in 2024 that the U.S. payments industry set up an independent information exchange framework to provide a single source for scam intelligence. Cross-industry data-sharing hubs enable a more comprehensive view of scam threats, better analysis, and more effective preventative measures.

C. New legislation should allow safe-harbor sharing of fraud-related information across industries, including the tech, social media, and telecommunications sectors. (The safe harbor provisions in the PATRIOT Act Section 314(b) currently apply only to financial institutions.)

Safe harbor protections exist in other areas of law to encourage sharing of threat information.

- The Cybersecurity Information Sharing Act of 2015 (CISA 2015), for example, provides liability protections for sharing cyber threat indicators and defensive measures among private entities and with the government.

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides a safe harbor allowing healthcare providers to share limited patient information on drug overdoses in emergencies without prior consent.

D. Create a data fusion hub. A central clearinghouse similar to the **National Center for Missing and Exploited Children** (NCMEC) could efficiently collect the appropriate data, enable quicker action to help victims, and serve as a one-stop shop for educating the public.

- In 1984, Congress passed the Missing Children's Assistance Act that established NCMEC. The Act authorized federal funding for the creation and operation of a private, nonprofit national resource center and clearinghouse to improve the management of cases involving missing and exploited children. It also serves as a hub for information sharing, training for law enforcement, and education of U.S. citizens.

- A similar organization dedicated to scam prevention could help the United States defend its citizens and financial institutions from attack by foreign cybercriminals.

In recognition of the rising threat of Transnational Organized Crime (TOC), we should think big and create a National Counter TOC Center in the executive branch. The Center would be an operational interagency effort, modeled on the successful National Counterterrorism Center that the US government created after 9/11. The National Counter TOC Center could be under DOJ and DHS, and it would comprise relevant elements from across the government and the private

sector. One of its key missions would be to address all of the ways we are being attacked by transnational criminals, including scams.

In recent months, the federal government has created a variety of task forces to address particular parts of the transnational crime threat. In June 2025, DOJ created a Health Care Fraud Data Fusion Center. In November 2025, DOJ created the Scam Center Strike Force to secure America against Southeast Asian cryptocurrency-related fraud and scams. A bill in the Senate with 41 cosponsors (S.1404 - Combating Organized Retail Crime Act) would create an Organized Retail and Supply Chain Crime Coordination Center in DHS.

Rather than pursue individual approaches, a White House coordinator and a National Counter TOC center would provide a more comprehensive and efficient response to the transnational organized crime threat.

3. Measure the problem. Good public policy requires good data

A. Congress should direct the Justice Department/Bureau of Justice Statistics (BJS) and Census Bureau to conduct statistically-valid household surveys to measure scam victimization. A government-sponsored national survey is important to accurately count victims and losses and determine the most common threat vectors. Scams are now among the most common crimes affecting Americans, but the last national fraud survey conducted by the U.S. Government was in 2017. Congress should provide the funds for annual fraud surveys, which is how the UK and Australia collect the appropriate data to focus their anti-scam strategies.

- The Pentagon and Department of Veterans Affairs should conduct surveys to measure scam victimization rates among the military and veteran population. A variety of data suggests that foreign adversaries deliberately target the US military and that military personnel and veterans suffer disproportionate losses compared to the civilian population.

B. The Government Accountability Office (GAO) should combine the siloed information on scams collected by the U.S. Government and create the first-ever national estimate of consumer fraud losses. (GAO released a report in March 2025 that estimates the amount of fraud losses to the U.S. Government, but it has not estimated losses to consumers.) GAO should also recommend ways to improve information collection and sharing across the government, which would be in keeping with the President's March 2025 Executive Order to stop waste, fraud, and abuse by eliminating information silos.

C. The US intelligence and law enforcement communities should produce an unclassified report that explains the nature of the threat that the United States faces from foreign organized crime, especially focusing on cybercrime that targets consumers and financial institutions. The report should address the identity, locations, and strength of foreign cybercriminals, and their methods and tactics. The government routinely produces such reports on drugs, ransomware, and other threats, but has never produced a comprehensive report on the threat faced by consumers and our financial institutions from foreign organized cybercrime.

4. Reduce fake advertising via improved authentication procedures

Criminals use fake advertising to entice victims to engage in fraudulent investments. The U.S. should respond by adopting common-sense authentication measures to ensure that financial ads can only be placed by legitimate businesses. Many American companies have agreed to institute measures to protect the citizens of other countries from fake advertising. These services should also be available in the United States.

- In the UK, Google says it has seen a "pronounced decline in reports of ads promoting financial scams" since 2021. That's when Google began requiring financial services advertisers to demonstrate that they are on a British government authorized list. Google now requires verification of financial services advertisers in 17 countries: Australia, Brazil, France, Germany, India, Indonesia, Ireland, Italy, New Zealand, Portugal, Singapore, South Korea, Spain, Taiwan, Thailand, and Turkey.

- Meta announced in 2024 that in the UK, financial ads must be authorized by the UK's Financial Conduct Authority before the ad is permitted on Meta's platforms. A similar policy is in place in Taiwan as of August 2024 and expanded to Australia in February 2025. Meta's policy includes insurance products, mortgages, loans, investment products and opportunities, and credit card applications.

- In Australia, nine major technology companies (Apple, Discord, Google, Meta, Snap, TikTok, Twitch, X and Yahoo) signed a voluntary industry code in 2024 that requires moving toward "reasonable measures to confirm that an advertiser holds the necessary financial services license to advertise a regulated financial service."

5. Proper labeling and blocking of scam phone calls and text messages

Many frauds succeed because it is relatively easy for criminals to manipulate the information displayed on a user's caller ID to show a false name or number that appears legitimate and trustworthy. They especially try to gain trust by pretending to be U.S. companies or Government officials in a telephone call or text message.

Many countries are deploying technology to reduce spoofing and the U.S. should do the same. Also, America leads the world in artificial intelligence. Surely we can detect and block the "package delivery" and "toll road" text message scams that are being perpetrated by Chinese cybercriminals. Google started filtering such scams on Android devices in March 2025, but other U.S. mobile device manufacturers have not followed suit.

A. Congress should direct the Federal Communications Commission (FCC) to swiftly implement measures to reduce the ability of criminals—especially foreign criminals—to impersonate legitimate U.S. businesses or the government. Since most scammers are foreign-based, scams would be reduced if Americans knew when they received a foreign phone call.

Dozens of countries around the world are employing technology to protect their citizens from spoofed international calls. (Example: A call from India that displays a U.S. number, or the name of a trusted company like Microsoft, Amazon, or a bank.)

Spoofed international calls: 22 countries now block inbound international phone calls that spoof domestic numbers. (UK, Australia, Sweden, Finland, Norway, Belgium, Latvia, Lithuania, Oman, Saudi Arabia, India, Singapore, Taiwan, Spain, Czech Republic, Ireland, Poland, Malta, Romania, Spain, Czech Republic, Italy.)

Three additional countries (Germany, Austria, Switzerland) do not allow an inbound international call to display a domestic number. Thailand marks incoming international calls with a "+" sign. These measures have achieved significant results by preventing foreign scammers from impersonating a domestic company.

Spoofed text messages: To prevent impersonation scams, five countries—UK, Australia, Singapore, Ireland, and Spain—have a capability for text messages to be authenticated. The sender IDs are registered, and only registered companies or organizations are able to display their name in the sender ID field of a text message.

- To prevent abuse of text messaging systems, Australia started allowing the senders of bulk text messages to register their SMS sender IDs on 30 November 2025. Registration of sender IDs is scheduled to become mandatory on 1 July 2026, after which unregistered sender IDs will be marked as "Unverified."

- The government of Singapore reported that scam texts fell by 70% within the first three months after it implemented its sender ID registry.

These or similar authentication measures must be used in the U.S. to protect our citizens from telecom-based attacks by foreign criminals who impersonate U.S. officials or businesses. According to the FTC, "Scams that impersonate well-known businesses and government agencies are consistently among the top frauds reported to the FTC."

B. The Truth in Caller ID Act of 2009 is antiquated and needs to be revised to keep up with the increased threat environment. The Act currently allows spoofing, as long as the spoofing is not done for fraudulent purposes. But it is very difficult for regulators to determine intent, so the Act is rarely enforced. A better approach would be to define certain calls as illegal, regardless of intent. Example: calls that use a spoofed area code or impersonate a business or government agency. It should be illegal to spoof a number that the caller does not have permission to use.

- In addition, the penalties in the 2009 Act have eroded with inflation, so they should be increased to deter scammers who pretend they are representing reputable companies.

6. Create a national capability to quickly take down malicious websites, especially fraudulent investment websites

Centralized data collection would allow the U.S. to quickly take down fake investment websites, which has proven to be an effective way to reduce fraud losses due to investment scams. The U.S. Government currently takes down some malicious websites, but our process is cumbersome and ad hoc. The U.S. Government does not collect or release comprehensive statistics about malicious website takedowns. Meanwhile, both Australia and the UK have created successful government programs and issue annual reports on their effectiveness.

- The Australian Securities and Investment Commission (ASIC) (the equivalent of the US Securities and Exchange Commission) has coordinated the removal of more than more than 14,000 investment scam websites and online advertisements since July 2023. ASIC removes an average of 130 malicious sites per week. Australia reports that investment scam losses decreased by 27 percent from 2023 to 2024. In the United States, the latest FBI/IC3 data show that losses to investment scams rose from $4.6 billion in 2023 to $6.6 billion in 2024—a 44-percent increase. ASIC recently announced that the investment scam website takedown capability is being expanded to include social media ads.

- In the UK, most website takedowns are done by the National Cyber Security Centre, an arm of GCHQ (equivalent to our National Security Agency). The UK created the Suspicious Email Reporting Service (SERS) in April 2020, which has proven to be a successful way of enabling the public and businesses to report suspicious emails, leading to the removal of thousands of scams. UK organizations and citizens send about 30,000 reports a day of suspicious emails and URLs. The result: 412,000 malicious URLs have been removed since 2020. The NCSC reports that 50 percent of these attacks were taken down within less than 1 hour. In addition, the median uptime for a cryptocurrency scam website is one hour, according to NCSC. As a result, the number of fake cryptocurrency scam websites found by the UK government has decreased dramatically since 2021.

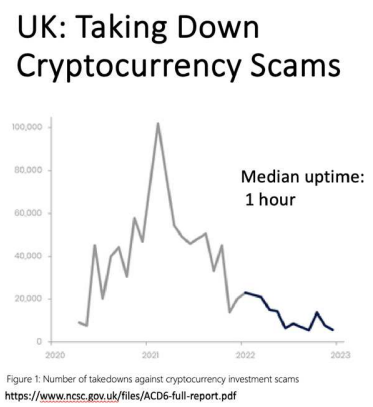


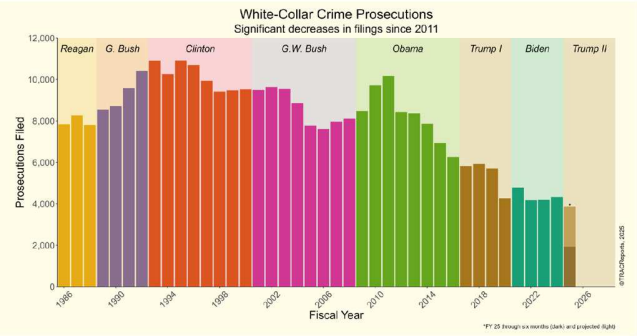
Figure 1: Number of takedowns against cryptocurrency investment scams
https://www.ncsc.gov.uk/files/ACD6-full-report.pdf

7. Boost law enforcement resources and intelligence priorities

U.S. law enforcement clearly lacks the resources to keep up with the tsunami of scams. Congress should bolster funding for investigators and provide adequate funds to improve scam training for law enforcement personnel. The UK announced in 2023 that it was adding 400 new investigators and ordering their intelligence community to "relentlessly pursue fraudsters wherever they are in the world."

In the U.S., because of resource constraints, less than 1/10th of one percent of fraud cases are investigated, according to testimony provided to the Senate Committee on Aging. The FBI initiated 3,020 attempts to freeze funds for victims in 2024. That is about 3/10th of one percent of the total number of complaints received by the FBI that year (859,532).

A recent study by Transactional Records Access Clearinghouse at Syracuse University shows that prosecutions of white-collar crime have declined 50 percent since 2014. The researchers conclude: "successive administrations of both U.S. political parties have deprioritized enforcing white-collar crimes."



8. Mount a focused government-industry effort to combat the "Tech Support Scam," the number one scam afflicting our senior population

The Committee should request that the Department of Homeland Security consult with industry partners and deliver a plan to significantly reduce the threat of the tech support scam. Measured by the number of victims, this scam is the number one scam affecting Americans over the age of 60—by far. The FBI's Elder Fraud Report shows this scam has more than double the number of victims than any other scam measured by the Bureau. The FBI's report says:

> *Call centers overwhelmingly target older adults, to devastating effect. Complainants over the age of 60 lost more to these scams than all other age groups combined, and reportedly remortgaged/foreclosed homes, emptied retirement accounts, and borrowed from family and friends to cover losses in these scams. Some incidents have resulted in suicide because of shame or loss of sustainable income. Tech/Customer Support and Government Impersonation are responsible for over $1.3 billion in losses.*

Total losses, including unreported, are far higher—perhaps exceeding $10 billion. Losses due to tech support/call center fraud are skyrocketing—more than doubling since 2021. Losses reported to the FBI from the tech support scam are more than 100 times the losses reported due to ransomware.

The U.S. mounted a significant effort to stop ransomware attacks starting in 2021, and the effort has seen considerable success. Like ransomware, the tech support scam is a technical cyberattack

that could be thwarted by technical countermeasures. The scam often involves "pop-ups" that are delivered by malicious online ads and the installation of remote access software. Some browser companies are beginning to use AI to detect the signature "pop-ups" that take over a person's computer, but these measures are not available by default. Another way to defeat the tech support scam is with better authentication of the origin of phone calls—the tech support scam collapsed in Finland when Finnish telcos started deploying measures to prevent caller ID spoofing from foreign calls.

9. Limits on crypto kiosks (crypto ATM machines) because of the harm to older Americans
In August 2025, the US Treasury Department issued a Notice warning about the skyrocketing growth of crypto ATM kiosks "for scam payments and other illicit activity." It notes that the FBI received more than 10,956 complaints reporting the use of such kiosks in 2024, with reported victim losses of approximately $246.7 million. This represents a 99-percent increase in the number of complaints and a 31-percent increase in reported victim losses since 2023.

Older Americans are bearing the brunt. According to FTC data, people aged 60 and over were more than three times as likely as younger adults to report a loss using a crypto kiosk. More than two of every three dollars reported lost to fraud using crypto kiosks was lost by an older adult.

The Treasury Department's Notice mentions that the speed and difficulty of reversing crypto ATM transactions make them an attractive payment mechanism for scammers. This generally differs from traditional bank or wire transfers where a payment transaction can remain pending for one to two days before settlement.

At least 40 states have introduced or pending legislation regarding cryptocurrency, digital or virtual currencies and other digital assets in the 2025 legislative session, according to the National Conference of State Legislatures. More than a dozen states have passed laws placing limits on payments and other states have proposed other legislation.

Because these machines are being used to defraud older Americans at scale, and the profits flow overseas to facilitate foreign organized crime, the time has come to place reasonable limits at the federal level to prevent abuse. A national framework with uniform standards across jurisdictions would help manage risks and build trust in digital currency investments.

The good news is that we can turn the tide. The UK and Australian governments have shown that, with an organized and adequately-funded approach, the United States would quickly save millions of victims and tens of billions in losses to the U.S. economy.

Thank you for the opportunity to submit this statement for the record. Stop Scams Alliance looks forward to working with the Committee on these important issues.

Respectfully submitted,

Ken Westbrook, Founder and CEO, Stop Scams Alliance
www.StopScamsAlliance.org

○