

**A D D E N D U M**  
**to**  
**SCAMMERS EXPOSED: PROTECTING OLDER  
AMERICANS FROM  
TRANSNATIONAL CRIME NETWORKS**

**This Addendum is available at:**

*<https://www.govinfo.gov/content/pkg/CHRG-119shrg61841/pdf/CHRG-119shrg61841-add1.pdf>*

**Submitted by Chair Grassley:**

Certified Threat Intelligence Analyst (CTIA), statement .....	2
Charlotte, Ayleen, statement .....	19
Department of Justice (DOJ), statement .....	22
Defense Credit Union Counsel (DCUC), letter .....	30
Love Said, Fraud Centre & Think Tank, The Science of Being Scammed: Why Romance Fraud Is More Than a Scam, statement .....	33
Stop Scams Alliance, statement .....	37

**Submitted by Ranking Member Durbin:**

America's Credit Unions, statement .....	50
Certified Threat Intelligence Analyst (CTIA), statement .....	2
Community Bankers Association of Illinois, statement .....	52

**Submitted by Senator Whitehouse:**

Romance scam artist from Nigeria who targeted RI widow going to prison, <i>The Providence Journal</i> , article .....	56
--	----

**Statement for the Record Submitted by CTIA**

**on**

**“Scammers Exposed: Protecting Older Americans from Transnational Crime Networks”**

**Before the**

**U.S. Senate Committee on Judiciary**

**June 17, 2025**



Chairman Grassley, Ranking Member Durbin, and Members of the Committee, on behalf of CTIA and the wireless industry, thank you for the opportunity to submit a statement for the record.

CTIA commends the Senate for its leadership in protecting Americans from the scourge of illegal and unwanted robocalls and robotexts, including scams targeted at older Americans. Thanks to Congressional action, the TRACED Act provided the Federal Communications Commission (“FCC”) with new tools to combat illegal robocalls and the Stop Senior Scams Act enabled the Federal Trade Commission (“FTC”) to forge new bonds among the wireless industry, consumer advocates, and financial institutions to help put a stop to bad actors who are intent on harming older Americans.

The wireless industry is helping lead the way in preventing these scams. Our actions work to protect consumers from scams on the voice and text platforms, including scams against older Americans. Today, we are advancing consumers’ control over the voice calls they receive and working to prevent the spam and scam calls that are a major consumer pain point. On the robotext front, the wireless industry is combatting billions of spam and scam text messages each month using innovative solutions that are helping prevent bad actors from corrupting the trusted environment of text messaging. We balance these steps with our ongoing support for legitimate calls and messages to help ensure that consumers get the communications they want.

Consumers rely on wireless more than ever before. This includes older Americans, who increasingly use wireless to stay connected with their communities and access financial,

health, emergency, and other essential resources increasingly available online. In fact, 94 percent of older Americans own a cellphone and are second only to 18 to 29-year-olds in reliance upon smartphones for access to the Internet and online services.

Unfortunately, bad actors target consumers, including older Americans, across a variety of platforms, including wireless and online services. Bad actors use social engineering tools and schemes to target consumers by impersonating trusted family, friends, financial institutions, and government agencies. As wireless providers use advanced tools and processes to prevent and swiftly stop scam and spam robocalls and robotexts, bad actors design their schemes to quickly move recipients from calls and text messages to websites or over-the-top (“OTT”) platforms beyond the reach of wireless providers.

Combating this problem requires a team effort among wireless providers, OTT service providers, financial institutions, consumer advocates, and law enforcement agencies. Efforts like CTIA’s Secure Messaging Initiative (“SMI”) and AARP’s National Elder Fraud Coordination Center (“NEFCC”) are bringing together resources from the private sector to aid law enforcement in investigating and prosecuting criminal fraud rings targeting older Americans. The Aspen Institute’s National Task Force on Fraud and Scam Prevention is also working to develop the first coordinated U.S. national anti-fraud strategy that builds upon industry-led partnerships with law enforcement to explore further collaboration and consumer education tools. CTIA is optimistic that our SMI and work by NEFCC and the Aspen Institute will further a holistic approach that can help state and federal law enforcement agencies to more efficiently “throw the book” at fraudsters.

Of course, there is more to do. And working together with members of this Committee, the FCC, the FTC, the U.S. Department of Justice (“DOJ”), state attorneys general, and our partners throughout the voice and text messaging ecosystems, we are making headway in fighting bad actors and maintaining consumer trust in voice services and text messaging.

### **The Wireless Industry Is Helping to Lead the Fight Against Robocalls.**

Although automated calls from banks, pharmacies, airlines, schools, and others can enhance consumer welfare, too many automated calls are intrusive. We all know the type – a call that comes with a robotic or familiar voice and an enticing offer or one that tries to scam us into disclosing personal data. And many of these are aimed at older Americans.

In response, wireless providers spearheaded the development of the STIR/SHAKEN framework years ago and led the way in implementing it, consistent with the directives of the bipartisan TRACED Act. STIR/SHAKEN helps identify callers and reduce caller ID spoofing as a key part of the industry’s multipronged defense against illegal and unwanted robocalls. Congressional adoption and the FCC’s implementation of the TRACED Act ensured this framework is now a critical component throughout voice networks, and STIR/SHAKEN has been a key step to restoring consumer trust in voice services.

Complementing STIR/SHAKEN, wireless providers and their ecosystem partners launched a range of powerful tools to regain consumer control over the calls they receive. These include strong know-your-customer practices, innovative call-blocking, tracing back illegal robocalls to identify bad actors, and robust robocall mitigation programs. AT&T’s

ActiveArmor, for example, features automatic fraud and spam call blocking and is included free with its plans. T-Mobile offers a variety of tools including Scam ID and Scam Block as well as a free Scam Shield app to help consumers identify and stop unwanted calls. Verizon engages in network-level blocking of highly-suspect traffic based on analytics and also offers Call Filter, an enhanced call labeling and blocking service, at no charge. In fact, wireless providers block, label, or identify over 45 billion scam calls each year while also working hard to support 2.4 trillion voice minutes last year. The FCC has recognized the success of these solutions and encouraged all voice service providers to take similar actions, such as using powerful analytic tools to complete legitimate calls and taking steps to block illegal calls.

CTIA and its wireless partners are embarking on the next generation of call authentication – Branded Calling. We know that the majority of calls from unknown numbers are not answered today, and consumers, including older Americans, are more likely to answer and engage with a call if they know the brand name of the caller. CTIA has developed a branded calling solution that leverages the STIR/SHAKEN framework to deliver trusted visual information to consumers’ smartphones that helps assure them that a call is coming from a verified source. This solution is called Branded Calling ID™ – or “BCID™.” BCID™ delivers verified, robust, and secure identity information including: (1) caller display name (e.g., “Home Depot”); (2) call logo; and (3) call reason (e.g., “Order Ready for Pickup”). With trusted, branded caller information, all consumers can make more informed choices about whether to pick up the phone, reducing the risk of being bothered by spam or scam calls.

Notwithstanding all of the solutions discussed above, we know that bad actor robocallers will continue to find ways to call consumers. To that end, wireless providers are key partners in USTelecom’s Industry Traceback Group (“ITG”) to identify, block, or take enforcement actions against bad actors. CTIA’s member companies and their partners across the voice ecosystem also continue to work to ensure that overseas counterparts take effective measures to mitigate foreign-originated illegal robocalls. Providers balance these steps with efforts to ensure that legitimate calls, including public safety calls, are protected.

These efforts have yielded promising results. In fact, according to ITG’s latest report, “[t]raceback-powered enforcement [has] led to sharp declines in numerous illegal robocall campaigns.” Robocall complaints to the FTC have also decreased steadily, reaching a six-year low in 2024. We are proud of this progress.

**The Wireless Industry Is Committed to Maintaining Consumer Trust in Text Messages.**

Today, wireless text messaging is one of the most popular and trusted forms of communication among American consumers. Americans exchanged 2.1 trillion text messages in 2023, and 90 percent of Americans use their phones to text at least monthly. The consumer trust that the wireless industry has built is why messaging boasts a 98 percent “open rate.” This is much higher than email, with a 20 percent open rate and 6 percent response rate. As these stats show, consumer trust in wireless text messaging remains high, and the wireless industry works collaboratively and innovatively to keep it that way.

As a result, CTIA and its member companies understand the importance of investing in proactive, multi-layered measures that include sophisticated tools, industry best practices, and public-private partnerships to protect consumers from spam and scam text messages.

At the outset, it is important to note that consumers' positive assessment of text messaging stems in part from the fact that messaging does not carry the same regulatory burdens as voice services. In contrast to voice services, where common carrier regulations impeded voice service providers from blocking unwanted robocalls, text messaging operates in a light-touch regulatory regime that has enabled wireless providers to be nimble and innovative in crafting solutions to protect consumers from a flood of spam and scam text messages. Wireless providers have not been forced to seek a government agency's permission to block or take action against illegal text messaging and bad actors; they do so proactively and aggressively to the benefit of consumers. And this has worked exceedingly well.

Wireless providers successfully prevent billions and billions of spam text messages from ever reaching consumers each year. In 2024 alone, wireless providers blocked more than 55 billion scam and spam robotexts. And blocking is only one part of the broader effort to make sure the wireless industry's playbook evolves to keep up with bad actors' changing tactics.

First, wireless messaging technologies and up-front vetting and verification practices help thwart bad actors before they can even send scam or spam text messages. As a threshold protection, wireless messaging technologies require valid originating information,

such as a legitimate telephone number. As a result, number spoofing has not plagued text messaging as it has with robocalling. Instead, impersonation scams – where bad actors try to trick consumers into thinking that a trusted entity like their bank is contacting them – have been more prevalent. To address this issue, wireless providers and their ecosystem partners require businesses and other message senders to disclose information about themselves and their campaign before they can send high volumes of text messages. This process has helped to weed out and prevent many bad actors from blasting out mass spam text messages.

Second, many different entities help make messaging work, both with respect to innovating messaging platforms and consumer protection. The messaging “pie” is expanding, including not only SMS/MMS text messaging offered by wireless providers, but also new platforms, like OTT, online and app-based messaging platforms, and recently-launched Rich Communications Service (“RCS”). Unfortunately, that also means that bad actors have more ways to target consumers, and their ambitions are not limited to any particular technology platform. All messaging providers – including RCS, OTT, and online platforms – will need to be part of the team effort to prevent spam messages and deter bad actors from targeting consumers through messaging.

Next, CTIA’s *Messaging Principles & Best Practices* (“*Best Practices*”) for the messaging ecosystem offer industry-led guidance to vindicate consumer preferences, while supporting innovative, legitimate communications. The *Best Practices* are widely adopted throughout the messaging ecosystem and focus on the key tenet of consent: Consumers should have control over the texts they receive, with the ability to opt-out at any time. Through these and

other principles, including those addressing privacy and security, the *Best Practices* help prevent consumers from receiving unwanted messages while promoting innovation that allows consumers to get the messages they do want.

CTIA is gratified that its efforts were recently recognized by a coalition of six national consumer advocate organizations:

[T]exting currently remains a valuable and trusted method of communication in the United States, largely because of the best practices developed by CTIA and adopted by its members and their partners. . . . [T]he entire texting ecosystem would be a disaster if fewer industry-developed restrictions against unwanted texts were applied.<sup>1</sup>

CTIA continues to update the *Best Practices* – for example clarifying who qualifies as a non-consumer sender to help ensure all types of entities understand what guidance applies to them as they set up their messaging campaigns.

Wireless providers and their messaging partners also deploy vast security and fraud prevention teams using the latest innovative technologies, machine learning and AI, and other spam mitigation tools to protect consumers through real-time analysis and other defense solutions. To enhance these protections, wireless providers have set up a common means for consumers to report unwanted text messages – 7726 (SPAM) – and partner with Apple and Google to make it easier for consumers to “Report Junk” directly through the wireless messaging applications that are built into most of our wireless phones. Wireless providers use this reported data to constantly evolve spam mitigation tools in real-time and keep pace with the constantly changing tactics of bad actors. And when wireless providers receive complaints about texts with suspicious URLs or domains, their teams investigate the

website to determine if the link is intended to support fraudulent efforts. If so, wireless providers can share that link with Google's Safe Search list so it can be blocked by most internet browsers.

The wireless industry and their messaging partners are constantly evolving and enhancing their tools, including by responsibly leveraging AI in myriad applications throughout the wireless ecosystem to prevent fraud, robocalls, and robotexts, strengthen cybersecurity, and more. CTIA and its member companies are mindful of both the benefits and risks of AI, and they are incentivized to strike the right balance in promoting innovative uses while fighting bad actors. We support the Administration's efforts to accelerate AI innovation through its AI Action Plan and AI R&D Plan, Congress' efforts to avoid a patchwork of state legislation on AI, and the FCC's bipartisan decision last year establishing clear guidance on the use of AI that has already helped the FCC and industry protect consumers from bad actors using AI voice-generating tools that fall within the scope of the Telephone Consumer Protection Act. We look forward to further developments like these that promote AI innovation rather than regulations focused on addressing AI-enabled robocalls and text messages.

Notwithstanding all of these tools, bad actors continue to seek out ways to get spam and scam text messages through to consumers, including older Americans. To complement industry tools and best practices, CTIA launched the SMI to help the FCC, FTC, DOJ, and other law enforcement agencies identify and go after bad actors. The SMI leverages the additional information available in the texting ecosystem (i.e., not just phone number and provider

name) that is not accessible in the voice context to help identify suspected bad actors and refer those to law enforcement for investigation. SMI participants also share suspected spam and scam messages and techniques to more rapidly and effectively shut down spam activity while targeting the senders of unwanted or fraudulent messages.

Through the SMI, we have already traced over 172,000 robotexts and made over a dozen referrals for enforcement actions to our partners at the FCC, FTC, DOJ, and the 50-state attorneys general enforcement task force. This included referrals focused on protecting older adults, such as a referral on a medical device scam that appeared to target seniors using chatbots and AI-generated voice calls. Collectively, these efforts are helping to enhance efforts to stop scammers and maintain consumer trust in wireless text messaging.

Congress, the FCC, the FTC, the DOJ, state AGs, and other authorities can contribute to this fight by encouraging industry efforts to coordinate and facilitate broad-based sharing of information about bad actors through CTIA's SMI. And enforcement authorities like the FCC, FTC, DOJ, and state AGs should prioritizing resources toward "throwing the book" at those that seek to harm consumers. The wireless industry is coordinating with federal and state authorities to stop bad actors, and more support for enforcement actions would further these efforts. And government and industry alike have a role to play when it comes to educating consumers on how they can protect themselves from scams, and encouraging broader adoption of industry best practices, including CTIA's *Messaging Principles and Best Practices* and industry vetting and monitoring tools, that enable the wireless industry to identify and stop bad actors.

CTIA and the wireless messaging ecosystem remain vigilant in seeking to combat scam and spam messaging, and we are pleased there was a nearly 40 percent drop in consumer complaints about text messages to the FCC and the FTC between 2021 and 2023.

Collaboration and information sharing across the wireless messaging ecosystem, cross sector- partners, and law enforcement agencies will help us continue to maintain consumer trust in wireless messaging by targeting bad actors and thwarting their evolving tactics.

### **The Wireless Industry Works Hard to Protect Older Americans from Scams and Fraud.**

Older Americans increasingly make use of wireless when it comes to connecting with family, friends, healthcare providers, banks, and more. Unfortunately, bad actors know this, too. As wireless providers use the tools and processes described above to prevent and swiftly stop scam and spam robocalls and robotexts, bad actors continue to evolve their schemes not just through robocalls and text messages, but often through websites or OTT platforms beyond the reach of wireless providers. Combating this problem requires a team effort among wireless providers, OTT and online service providers, as well as other sectors like financial institutions, consumer advocates, and law enforcement agencies.

One such example of cross-sector collaboration is the Aspen Institute's National Task Force on Fraud and Scam Prevention. The Aspen Institute is convening hundreds of experts to develop a national strategy to combat transnational criminal enterprises abusing American financial systems, social media, communications, and retail platforms to defraud consumers, including older Americans.<sup>2</sup> The Aspen Institute recently found that the private sector is meaningfully investing in anti-fraud efforts, and reporting and information sharing between

the private sector and law enforcement should be a focus to catch and stop criminal operations at scale.<sup>3</sup> This is where CTIA's SMI and the NEFCC are focusing by facilitating actionable information sharing among the private sector and law enforcement agencies to break up criminal fraud rings, particularly criminal operations that target older Americans.<sup>4</sup> CTIA is optimistic that our SMI and the work of NEFCC and efforts like the Aspen Institute will further a holistic approach that can help state and federal law enforcement agencies to more efficiently "throw the book" at fraudsters.

We are also engaged in new partnerships to enhance cross-sector collaboration that can stop bad actors targeting older Americans. For example, CTIA recently led a working group that was formed by the FTC as part of Congress' direction in the Stop Senior Scams Act, which focused on combating robotext fraud targeting older adults. As a result of this effort, wireless providers and financial institutions are engaged in a collaborative dialogue about how sharing actionable information can stop bad actors. For example, the Financial Services Information Sharing and Analysis Center ("FS-ISAC") has found that a financial institution sharing actionable information with wireless providers led to a 90 percent reduction in consumer reports of receiving scam texts.<sup>5</sup>

In addition to collaboration across sectors and with law enforcement, another key pillar of anti-fraud efforts is consumer education, particularly for older Americans. CTIA's Consumer Resource pages, as well as member company websites, offer guidance for how consumers, including seniors, can protect themselves from scams. And educational campaigns, like AARP's "Pause. Reflect. Protect." And the American Bankers Association

“Banks Never Ask That,” are helpful tools that complement industry resources and help reach a wider audience. These resources as well as others, such as AARP’s Fraud Watch Network™, provide consumers with meaningful steps to report scams. The FCC and FTC also publish alerts that encourage consumers to spot and avoid common scams, like “Grandparent” scams, romance scams, and identity theft.<sup>6</sup>

Protecting older Americans from robocall and text messaging scams is a priority for the wireless industry. Of course, there is more that we can do, together.

**Congress Should Consider Ways to Boost Efforts to Fight Robocalls and Robotexts.**

The TRACED Act was landmark legislation that encouraged the adoption of innovative technologies and solutions that are making a meaningful impact on reducing the volume of illegal robocalls. The Stop Senior Scams Act is enhancing collaboration across private industry sectors and partnerships with government agencies to prevent bad actors that aim to defraud older adults. CTIA offers a few suggestions on how this Committee can build on these positive frameworks to continue to address the enduring problem of robocalls and robotexts.

First, we support the Administration’s efforts to do more to protect consumers and our voice and text ecosystems. As FCC Chairman Brendan Carr noted in his first Commission-level action as Chair, “[c]racking down on illegal robocalls will be a top priority at the FCC.”<sup>7</sup> And FTC Chairman Andrew Ferguson has noted that “[r]obocalls continue to vex consumers and remain a scourge, but . . . the FTC’s efforts have gone a long way to improving quality of life for

Americans who want an end to vexatious calls.”<sup>8</sup> We support ongoing and renewed efforts by federal and state law enforcement agencies to deter bad actors and protect consumers.

The FTC’s efforts to adopt and enforce new rules that address the increasing use of impersonation fraud, including scams fueled by AI and other advanced technologies, while protecting legitimate business activities, are also putting bad actors on notice. The FTC has taken action to stop fraudsters impersonating government agencies and businesses. We support the FTC taking the next step to target fraudulent impersonation of individuals while being careful to ensure that any new rules are properly targeted at bad actors and not the platforms or services abused by those bad actors. Congress could also consider whether criminal laws and penalties are specifically targeted at impersonation fraud to give law enforcement agencies the tools they need to deter bad actors while permitting legitimate uses of communications technologies. No grandparent should be defrauded for sincerely believing they are trying to help their grandchild.

In addition, Congress could support efforts to establish a national strategy to combat scams and fraud. As the Aspen Institute Anti-Fraud Task Force members recognize, we need a unified, whole-of-government approach that elevates fraud as a policy and enforcement priority. Creating a task force or similar centralized framework would provide stakeholders with a clear point of contact, improve coordination across sectors, and help enforcement against bad actors.

Congress could also amplify consumer education efforts through a national campaign that helps ensure consumers, particularly older adults, are armed with the information they

need to protect themselves against scams. By elevating existing guidance like AARP’s “Pause. Reflect. Protect.” to a national level, the administration can promote efforts to empower and educate consumers, and in turn protect them from fraud.

Finally, we value our partnerships with law enforcement and encourage Congress to take steps to promote more action against the bad actors behind illegal robocalls and robotexts. There are both federal and state agencies working to fight consumer fraud, but many lack the personnel or resources to bring cases. Congress could have agencies report on their current consumer fraud resources and actions and leverage that information collection to identify areas that could use more support. By prioritizing resources for enforcement at the federal and state levels, Congress can help take more bad actors off the field and stop illegal robocalls and robotexts at the source.

\* \* \*

The wireless industry is proud of our efforts to reduce the volume of illegal robocalls and prevent spam and scam text messages from reaching consumers. We know there is more work to do to protect consumers, and with the support of this Committee, the wireless industry can continue to lead in mitigating efforts by bad actors. We look forward to working with you to continue to protect consumers from intrusive and illegal robocalls and robotexts.

---

<sup>1</sup> Letter from Margot Saunders, Senior Counsel, National Consumer Law Center et al., to Marlene Dortch, Secretary, FCC, CG Docket No. 21-402 et al., at 2 (filed Mar. 6, 2024).

<sup>2</sup> *Developing a National Strategy to Safeguard Against Fraud and Scams*, ASPEN INSTITUTE FINANCIAL SECURITY PROGRAM, <https://fraudtaskforce.aspeninstitute.org/> (last visited June 10, 2025).

<sup>3</sup> *Phase One Working Group Outputs*, ASPEN INSTITUTE FINANCIAL SECURITY PROGRAM (May 23, 2025), <https://fraudtaskforce.aspeninstitute.org/phase-one-outputs>.

---

<sup>4</sup> National Elder Fraud Coordination Center, <https://www.fightelderfraud.org/> (last visited June 10, 2025); Press Release, AARP, AARP, Amazon, Google, and Walmart Support Launch of New Initiative to Combat Elder Fraud (Apr. 16, 2025), <https://press.aarp.org/2025-04-16-AARP,-Amazon,-Google,-and-Walmart-Support-Launch-of-New-Initiative-to-Combat-Elder-Fraud>.

<sup>5</sup> *Stop the Scams: A Phishing Prevention Framework for Financial Services*, FS-ISAC (Nov. 2024), <https://www.fsisac.com/hubfs/Knowledge/Phishing/StopTheScams-APhishingPreventionFrameworkForFinancialServices.pdf>.

<sup>6</sup> ‘Grandparent’ Scams Get More Sophisticated, FCC (Mar. 6, 2025), <https://www.fcc.gov/consumers/scam-alert/grandparent-scams-get-more-sophisticated>; *Addressing Scams Affecting Older Adults*, 6, 2025), <https://www.fcc.gov/consumers/scam-alert/grandparent-scams-get-more-sophisticated>; *Addressing Scams Affecting Older Adults*, FTC, <https://consumer.ftc.gov/features/addressing-scams-affecting-older-adults> (last visited June 10, 2025).

<sup>7</sup> Press Release, FCC, First Commission-Level Vote Under Chairman Carr Proposes A Nearly \$4.5 Million Fine Stemming From Apparently Illegal Robocall Scheme (Feb. 4, 2025), <https://docs.fcc.gov/public/attachments/DOC-409354A1.pdf>.

<sup>8</sup> Andrew N. Ferguson, Chairman, Federal Trade Commission, Testimony before the Committee on Appropriations, Subcommittee on Financial Services and General Government (May 15, 2025).

## WRITTEN STATEMENT FOR THE UNITED STATES SENATE

*Submitted by Ayleen Charlotte*

Date: 06-10-2025

Subject: Fraud, Institutional inaction and the **URGENT** need for systemic change

Chairpersons, Honorable Members of the Senate,

Thank you for the opportunity to submit this written statement.

Let me begin by saying: I would have preferred to be here in person today, to look you in the eye and tell you my story directly. Unfortunately, even six years after I was defrauded, I am still living with the financial consequences. I continue to survive on a limited budget and simply cannot afford to fly to the United States to speak to you face-to-face. That fact alone reveals something critical: fraud is not just a moment of deception. It is a trauma with long-term, life-altering consequences. And victims, like myself, are still paying the price financially, emotionally, and socially years after the crime was committed.

My name is Ayleen Charlotte. In 2022, the world came to know my story through the Netflix documentary *The Tinder Swindler*. In it, I shared how I, and others—were manipulated and financially devastated by a professional con artist who pretended to be a wealthy businessman seeking love.

The documentary exposed a serious and global issue: romance fraud. However, it also gave the impression that only women were affected. That's a harmful misconception. The truth is, **everyone who crossed paths with this man was in danger of being exploited**—men, women, companies and organizations. I have spoken to people of all genders, all backgrounds, and all continents who were defrauded by him. In the United States alone, multiple legal complaints have been filed against him. This is not a personal drama it is organized, international crime. And it's happening at scale.

---

### 1. A Society That Fails Its Victims

After discovering the fraud, I did what any responsible citizen would do: I sought help. I went to my bank. I contacted the companies that facilitated the scam. I spoke to law enforcement. I even sat down with the FBI and handed them all the evidence I had, every document, conversation, name and bank trail.

And yet... nothing happened. No meaningful investigation. No updates. No justice.

Instead of being supported, I was judged. Instead of being believed, I was questioned. I was turned away again and again, as though the crime committed against me was, somehow it was my fault.

This is not just my experience. It is the experience of thousands—perhaps **millions**—of fraud victims. They are treated with suspicion, not compassion. Shame, not support. Our systems are not built to help victims; they are built to process cases. And if your case doesn't fit neatly into a traditional box, it is often ignored.

Worse still, victim blaming is rampant. We live in a society that asks, “*Why did you fall for it?*” instead of “*Why was this person allowed and able to do this?*” When we focus on what victims “should have known,” we shift the attention away from the criminals who planned and executed the fraud. And when we do that, we always let the criminals win.

---

## 2. The Role of First Responders: Make or Break

We must understand the enormous responsibility that rests on the shoulders of **first responders**: the bank employee who takes the first call, the police officer who files the report, the fraud team agent who reads the statement. These are not small interactions—they can define a victim’s entire recovery process.

The way someone is treated in those first hours or days can either help them begin to heal—or deepen their trauma. It can give them the strength to fight—or push them into silence. I know victims who found hope because a single person believed them. I also know victims who spiraled into depression or even considered or committed suicide because they were dismissed, mocked or told it was their own fault.

This is why systemic change is not just about policies. It’s about **training, empathy and accountability** at every level—especially in frontline roles.

## 3. Silence Is Permission

I want to be absolutely clear: **when authorities stay silent, they give criminals permission to continue.**

If a con artist can move from country to country, scamming people across borders without consequence—if even the FBI won’t act despite evidence—then the message is clear: these crimes are low priority. And fraudsters know it.

Online scams are often treated as “less serious” than physical crimes. But the emotional, psychological and financial damage is just as real—sometimes more so. It’s invisible, prolonged, and often deeply isolating. The lack of prosecution doesn’t just fail current victims; it invites new ones.

---

## 4. A Call for Cultural and Structural Change

If we as a society do not change our approach to fraud, we will continue to empower the criminals and re-traumatize and silence the victims.

We need to stop asking “*Why did the victim fall for it?*” and start asking “*How do we stop this from happening again?*”

We must:

- Mandate trauma-informed training for all first responders—banks, law enforcement, customer service, and fraud departments.
- Hold platforms and companies accountable for enabling or ignoring fraud on their systems.
- Establish clear, enforceable timelines for investigations and updates for victims.
- Provide financial, legal, and psychological support services tailored to the needs of fraud victims.
- Fund awareness campaigns that reduce stigma and break the silence around online fraud.
- Prioritize international cooperation to track and prosecute fraudsters across borders.

Because **every time we focus on blaming victims, we let the criminals walk free.**

---

## **5. Final Words: When Will We Take This Seriously?**

I did not ask to be scammed. I did not choose to be manipulated. But I AM choosing to speak out. And I am doing it not just for myself, but for the millions who can't. Because they are too ashamed, too afraid that no one will believe them or too depressed to keep fighting.

The truth is: I am still recovering. I am still rebuilding my life—financially, emotionally, and socially. But I have learned one thing above all else: silence protects the fraudsters, and shame silences the victims.

So today, I ask this Senate to be part of the solution. To stand with victims. To take action. To send a clear message—not just across the U.S., but around the world—that **fraud is a crime, victims deserve justice and criminals will be held accountable.**

Because let us not forget: **fraud now accounts for 45% of all crime worldwide. Forty-five percent.**

So I ask you: **When will we—as a global society—finally take this seriously?**

Thank you for listening.

**Respectfully submitted,**  
Ayleen Charlotte  
[ayleen@ayleencharlotte.com](mailto:ayleen@ayleencharlotte.com)

+ 31627496143



# Department of Justice

---

**STATEMENT FOR THE RECORD**

**BEFORE THE  
COMMITTEE ON THE JUDICIARY  
UNITED STATES SENATE**

**FOR A HEARING ENTITLED  
SCAMMERS EXPOSED: PROTECTING OLDER AMERICANS FROM  
TRANSNATIONAL CRIME NETWORKS**

**PRESENTED**

**JUNE 17, 2025**

## **Statement for the Record**

**Before the Committee on the Judiciary  
United States Senate**

**At a Hearing Entitled  
Scammers Exposed: Protecting Older Americans from Transnational Crime Networks**

**Presented  
June 17, 2025**

Transnational fraud schemes, such as fraudulent cryptocurrency investment schemes, romance scams, technical support scams, lottery fraud, and government imposter schemes, present a dire threat to the financial and emotional health of the American public. Transnational fraud schemes originate in various countries around the world and victimize Americans in every corner of the nation. Victims are of all ages, but when seniors lose money, they often lose considerably more and have little chance of recovering from their losses.

The Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3), which collects reports and enables investigations of cyber and cyber-enabled crimes, issued its yearly report on April 23, 2025. The amounts of losses continued to rise sharply in 2024. Losses due to cyber-related crimes reported to IC3 rose to over \$16.6 billion, which represents a 33% increase in losses over 2023. In 2024, the Federal Trade Center's consumer complaint database received reports from consumers of more than \$12.5 billion lost to various frauds, a 25% increase from the previous year.

According to a Financial Crimes Enforcement Network (FinCEN) report issued in 2024, financial institutions reported approximately \$27 billion in elder financial exploitation suspicious activity between June 2022 and June 2023. Most of the reports involved elder scams, where victims were deceived into transferring money to imposters. The FBI's IC3 also produces an annual report specifically on elder fraud (see 2024 IC3 Elder Fraud chapter in the Federal Bureau of Investigation Internet Crime Report 2024, [https://www.ic3.gov/AnnualReport/Reports/2024\\_IC3Report.pdf](https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf)) at both the national and state levels. In 2024, the IC3 received 147,127 complaints from people self-reporting as over 60 years of age, which is a 46% increase from 2023. Reported losses exceeded \$4.8 billion, which is a 46% increase from 2023. Reported losses exceeded \$4.8 billion, which is a 43% increase from 2023. Within those losses, 7,500 complainants lost over \$100,000, and the average loss was \$83,000.

These statistics drastically underestimate the prevalence of fraud, given the documented underreporting of financial schemes. Although not all fraud reports counted in the statistics specify that the offenses were committed across borders, federal investigations consistently reveal that the

most prolific schemes both have a foreign origin and are committed by transnational criminal organizations.

According to a 2023 Gallup poll, 15% of Americans reported that at least one member of their household has fallen prey to a financial scam. They reported that less-educated and lower-income adults fall prey most. Fifty-seven percent of Americans say they frequently or occasionally worry about being victimized by a scam.

### Overview

Combatting and preventing elder fraud remains one of the Department's priorities. Federal prosecutors and law enforcement agents across the country work to identify fraudsters and bring them to justice. Some recent examples are provided below:

- A federal jury convicted Florida resident of operating a mass mailing fraud scheme that used transnational infrastructure to target elderly and vulnerable victims.
- A Jamaican national who was extradited from Jamaica was sentenced in federal court in Scranton, Pennsylvania, to 84 months in prison for his role in a fraudulent sweepstakes scheme that targeted older victims in the United States.
- A Nigerian national who was extradited from Portugal was sentenced to 97 months in prison for his role in a transnational criminal organization that operated an inheritance fraud scheme targeting elderly U.S. consumers.
- Two Southern California Men were arrested on an indictment alleging a scheme to launder money for a variety of transnational elder fraud schemes.
- Twenty-five Canadian nationals were charged in connection with a nationwide multimillion dollar “grandparent scam” in which they falsely claimed an elderly victim’s relative urgently needed money for various reasons.
- The FBI, through its Operation Level-Up, has saved victims an estimated \$366 million as of May 2025 by warning specific individuals that they are involved in cryptocurrency investment fraud schemes, and thereby preventing further investment in the schemes.
- As of April 2025, the Department’s Consumer Protection Branch and the U.S. Postal Inspection Service have returned over \$105 million to victims in cases against data companies that supplied transnational elder fraud schemes with the names of victims to defraud.
- A collaboration among the Department’s Consumer Protection Branch, FBI, and Indian law enforcement in the area of cyber-enabled financial crimes and transnational call center fraud has enabled over 215 arrests in India through 11 joint operations in 2024.
- 

### 2024 Elder Justice Report’s Key Statistics

The most recent Annual Report to Congress on Department of Justice Activities to Combat Elder Fraud and Abuse (<https://www.justice.gov/elderjustice/media/1374366/dl?inline=>), submitted in October 2024 as required by the Elder Abuse Prevention and Prosecution Act

(EAPPA), reflects the Department’s many elder justice efforts from June 2023 to July 2024. During that reporting period, the Department:

- Pursued over 300 enforcement actions against 700 defendants charged with stealing nearly \$700 million from over 225,000 older Americans;
- Returned millions of dollars to victims of elder fraud schemes and worked with financial institutions to freeze over \$27 million on behalf of older victims before those funds were transferred to fraudsters;
- Conducted nearly 1000 elder justice events and trainings around the country to raise public awareness of elder abuse and fraud schemes;
- Bolstered the efforts of state, local, and Tribal organizations, including elder abuse multidisciplinary teams and Elder Justice Coalitions, to better serve older adults; and
- Supported older victims and their families through the National Elder Fraud Hotline, which received over 50,000 calls during the reporting period and helped older victims to report potential crimes and locate available resources and services.

#### DOJ’s Approach

The Department of Justice employs a multifaceted approach to combating transnational fraud, including elder fraud. We are vigorously pursuing perpetrators of transnational scams. Many of the Department’s cases involve perpetrators of scams that began overseas, including fraudulent cryptocurrency investment schemes, romance scams, technical support scams, lottery fraud, and government imposter schemes.

The Civil Division’s Consumer Protection Branch helps to coordinate the Department’s efforts against transnational elder fraud schemes, including by bringing both criminal and civil cases. Cases are also brought by U.S. Attorney’s Offices across the country. Key to the Department’s efforts are our outstanding partners, including federal law enforcement, like the FBI, Homeland Security Investigations, U.S. Postal Inspection Service, and U.S. Secret Service, as well as foreign law enforcement and state and local counterparts.

Many fraudsters run “imposter” schemes, pretending to be the government or a private entity like a bank, tech company, or retailer. These fraud schemes, which generally threaten severe consequences like arrest or loss of someone’s entire savings if money is not received, prey on fear.

Some fraudsters pretend to be a romantic interest, in what are called “romance scams.” These scams occur when fraudsters use a fake online identity to gain victims’ affection and trust. The scammers then use the illusion of a romantic or close relationship to manipulate and steal from the victims, many of whom are elderly.

The Department also is pursuing cases against perpetrators of “grandparent scams.” “Grandparent scams” are particularly pernicious versions of imposter scams. Call recipients are told that a family member is in immediate jeopardy—for example, that they have been arrested or are dangerously ill—and urgently need money. Fraudsters frequently try to isolate their victims by

concocting some reason the victim cannot consult with friends, family, or law enforcement—such as saying the case is under a “gag order.”

The Department is taking a multipronged approach that uses every tool at our disposal. Where possible, we file charges against foreign perpetrators and bring those perpetrators to the United States through the extradition process to face justice in our courts. At times, however, bringing foreign perpetrators to the United States is not practicable. For example, in some cases, the process would take decades. In those situations, we work with foreign law enforcement to assist with the prosecution of fraudsters in the country where they are located and from which they committed the crimes. The Department and FBI have developed channels of communications with law enforcement in countries such as India and Ghana specifically for the purpose of sharing information on transnational fraud schemes, and to encourage police forces to shut down call centers and arrest perpetrators. The Department also pursues civil forfeiture of the illicit proceeds of these scams when appropriate, including when criminal prosecution is unlikely or impossible.

Foreign scams often rely on assistance from individuals located in the United States. For instance, a fraudster placing a large volume of phone calls may need to use a U.S.-based telephone network. Individuals located in the United States may help launder money stolen from victims, including through the transfer of gift cards purchased by victims at the direction of fraudsters located abroad. The Department has prosecuted people providing these types of services, which form part of the essential infrastructure of these fraud schemes.

One method by which fraudsters move money from victims in the United States to foreign bank accounts is through people (sometimes described as “money mules”) who may have no idea that they are facilitating the theft of someone else’s money. At times, fraudsters will convince victims to receive funds from people the victims do not know (but who are, in fact, other fraud victims) and then instruct the victims to forward that money to other members of the scheme. The person sending the money may think they are helping a friend overseas or that someone is helping them pay taxes on a lottery prize, but, in reality, the person sending the money is unwittingly facilitating international fraud.

Some “money mules” begin as victims and subsequently are persuaded to transfer money sent to them by other victims. Some of those individuals may be entirely unaware that their conduct fuels fraud, while others eventually come to understand the nature of the activity (or remain willfully ignorant). The Department’s Consumer Protection Branch has spearheaded efforts to combat fraudsters’ reliance on money mules. Much of this activity involves warning individuals who may not be aware they are facilitating fraud.

The Department is increasingly seeing organized crime, including cartels and gangs, operating fraud schemes targeting older adults. We are taking some of the strategies and tools we have used in investigating drugs and violent crime—including, for example, the Racketeer Influenced and Corrupt Organizations statute—and making sure that our fraud prosecutors and agents are considering the use of those same tools and employing them where appropriate.

The Department also has been increasing its use of data analytics. For example, when seeking to identify the most pervasive schemes impacting older adults or involving public funds,

the Department uses the data at its disposal to ensure that investigators and prosecutors spend their resources on the most harmful schemes. The Department also regularly reviews information provided by financial institutions and reports made by consumers to find the most harmful consumer schemes.

Another strategy is disruption. We recognize there are times when investigations will, of necessity, be lengthy and may not quickly lead to arrests. In some cases, where warranted and appropriate, we may seek to disrupt fraud schemes by preventing them from using their established websites, telephone numbers, and bank accounts, and thereby force scammers to spend resources to rebuild the infrastructure they rely upon to operate. When fraudsters are forced to devote time and money to adjust their operations as a result of targeted law enforcement action, that is time and money they are unable to devote to victimizing consumers. In some other cases, when possible, we may even freeze and return stolen funds for victims of fraudulent domestic and international transactions. The FBI's IC3 Recovery Asset Team (RAT) streamlines communications between FBI field offices and financial institutions and was specifically established to initiate Financial Fraud Kill Chain requests and freeze stolen funds.

The Department's Transnational Elder Fraud Strike Force is comprised of 20 U.S. Attorney's Offices, in addition to the Consumer Protection Branch. The Strike Force works closely with dedicated law enforcement partners, including the FBI, the U.S. Postal Inspection Service, and Homeland Security Investigations, to identify, investigate, disrupt, and prosecute the largest and most harmful elder fraud schemes operating across the globe. They coordinate with foreign law enforcement to bring perpetrators to justice and, where possible, disrupt the infrastructure used by multiple fraud schemes. They also prosecute those individuals located in the United States responsible for facilitating foreign scams.

Supplementing the Strike Force, U.S. Attorney's Offices across country have developed their own approaches to addressing elder fraud within their respective districts. The San Diego Elder Fraud Task Force is an excellent example of how federal, state, and local law enforcement can develop a strategy to work together. Indeed, one of the greatest successes from the San Diego Task Force came through partnership with the Consumer Protection Branch to shut down a nefarious grandparent scheme that instilled fear in elderly individuals by telling them that money was required to bail their grandchild out of jail. Perpetrators were charged with operating a racketeering enterprise, convicted, and sentenced to prison for their crimes. The Task Force is comprised of a team of dedicated federal agents and state law enforcement officers. They routinely provide training and education to local law enforcement on elder fraud scams, conduct public outreach to raise awareness about the dangers of these scams, and coordinate with financial institutions to ensure that they are watchful for—and appropriately report—potential frauds. They also investigate the elder fraud crimes occurring within the district so that criminals responsible can be prosecuted. Prosecutions occur both at the state and federal level, depending on the size and scope of the fraud. In addition to the Task Force's work investigating and prosecuting ongoing elder fraud and preventing future elder frauds, it has also undertaken a successful operation to recover funds fraudulently obtained.

Prosecutors and agents across the country have been seeking to combat the increased use of fraudulent cryptocurrency schemes targeting the elderly. The Elder Fraud chapter of the Federal

Bureau of Investigation Internet Crime Report 2024 captured 33,369 complaints specifically related to cryptocurrency from people that self-reported as over 60 years of age. The losses reported totaled \$2,839,333,197 dollars. Cryptocurrency can be used as a form of “payment.” For example, during a government imposter scam or romance scam, a fraudster may ask the victim to provide them with funds via a cryptocurrency exchange or a cryptocurrency ATM. Cryptocurrency can also be part of the fraud “pitch” made to victims, in which a fraudster will try to convince a victim to invest in cryptocurrency. But that “investment” is not real; rather, the fraudster simply takes the victim’s money and disappears. As stated above, the FBI, through its Operation Level-Up, has saved victims an estimated \$366 million as of May 2025 by warning specific individuals that they are involved in cryptocurrency investment fraud schemes and thereby preventing any further investment in those schemes.

The use of artificial intelligence (AI) also increases the effectiveness of fraudsters’ scam attempts. Deep fake videos of celebrities and cloned voices of loved ones make it more challenging for the public to identify scams. Perpetrators also use AI to vary the content of their email and text message blasts to the public to evade spam filters. The Department and its partners are actively investigating schemes using these techniques.

The importance of reporting suspected fraud cannot be overstated. Not every report will result in a prosecution or the return of stolen funds. But none of our cases could be developed without victims coming forward and sharing their experiences with law enforcement. Even when a victim report does not lead to a prosecution, the information provided can help us learn how fraudsters are operating. We use victim reports to advise the public about new ways a fraudster might try to convince someone to give them money.

One such resource for victims of elder fraud is the National Elder Fraud Hotline at 1-833 FRAUD-11 (1-833-372-8311). This hotline, managed by the Department’s Office for Victims of Crime (OVC), is staffed by experienced professionals who provide personalized support to callers by assessing the needs of the victim and identifying next steps. Case managers will identify appropriate reporting agencies, provide information to callers to assist them in reporting or connect them with agencies, and provide resources and referrals on a case-by-case basis. The hotline is staffed five days a week from 10:00 a.m. to 6:00 p.m. ET. English, Spanish, and other languages are available.

#### Additional Departmental Elder Justice Efforts

As required by the Elder Abuse Prevention and Prosecution Act, the Department also develops trainings, resources, tools, and information for elder justice professionals, including those who provide services to victims of transnational fraud schemes. For example, the Department has developed trainings for law enforcement on how to identify and investigate elder abuse and financial exploitation, conduct forensically sound interviews with older adults, and collaborate with other elder justice professionals in their communities. To highlight these resources, the Department hosted the first National Elder Justice Law Enforcement Summit, which brought together representatives of state and local law enforcement organizations from all 50 states and the District of Columbia to share best practices, resources, and tools to combat elder abuse and fraud.

For state prosecutors, the Department developed trainings on how to investigate and prosecute elder abuse, and the important role that decision-making capacity plays in both criminal and civil cases. Those trainings included the Department's Elder Justice Decision-making Capacity Symposium, where subject matter experts discussed the expected changes in the aging brain and their potential impact on decision-making, available tools and protocols for assessing an older adult's decision-making capacity, and the impact on guardianship proceedings, criminal prosecutions, and civil legal remedies of an assessment of an older adult's decision-making capacity.

The Department has also developed resources and trainings for judges, including the Guardianship Evaluation Toolkit, which was designed by subject matter experts in order to help judges gather the relevant information to determine whether a guardianship needs to be imposed, or whether a less restrictive alternative may be appropriate.

All of the Department's trainings and resources are available for free on the Department's Elder Justice Website ([www.elderjustice.gov](http://www.elderjustice.gov)).



**DCUC**  
DEFENSE CREDIT UNION COUNCIL

1627 Eye St, NW  
Suite 935  
Washington, DC 20006

202.734.5007  
www.dcuc.org

**Jason Stverak**  
Chief Advocacy Officer

June 16, 2025

The Honorable Chuck Grassley  
Chair, U.S. Senate Committee on the Judiciary  
135 Hart Senate Office Building  
Washington, D.C. 20510

The Honorable Dick Durbin  
Ranking Member, U.S. Senate Committee on the Judiciary  
711 Hart Senate Office Building  
Washington, D.C. 20510

**Re: Hearing on “Scammers Exposed: Protecting Older Americans from Transnational Crime Networks”**

Dear Chairman Grassley and Ranking Member Durbin:

On behalf of the Defense Credit Union Council (DCUC) and its member credit unions that proudly serve America’s uniformed service members, veterans, civilian defense employees, and their families, we write to commend the Committee’s focus on exposing and combating the international criminal networks that prey on older Americans. These threats strike at the heart of the communities our institutions are committed to defending—on the battlefield and in their financial lives.

DCUC represents over 200 defense credit unions serving more than 40 million members and stewarding more than \$525 billion in assets. Our members include many of the nation’s most trusted financial institutions on military bases and VA campuses, and we take our role in protecting older Americans and vulnerable veterans seriously. Many of the scams identified in this hearing—from romance fraud to phishing schemes to cross-border money laundering—directly target our members, especially older veterans living on fixed incomes or survivors of service-connected disability recipients.

**The Unique Protective Role of Defense Credit Unions**

**1. Advanced Fraud Detection and Member Monitoring**

Defense credit unions have developed sophisticated anti-fraud detection systems specifically calibrated for military and veteran member patterns. These systems flag anomalous transfers, frequent international transactions, and behavioral changes that may indicate undue influence—particularly among older members. When flags are raised, member service teams immediately intervene to stop payments, reverse charges, or freeze accounts as appropriate.

## 2. Preventative Financial Education Programs

We deliver tailored fraud education to older members through in-person seminars at military installations, virtual classes for retirees, and targeted email/text alerts. These efforts help prevent common scams such as grandparent fraud, fake VA benefits calls, and “tech support” ruses before they happen. Some defense credit unions also conduct family outreach campaigns to educate caregivers and spouses.

## 3. Advocacy and Legislative Partnerships

DCUC has repeatedly urged Congress to prioritize scam prevention and support institutions like ours in fraud interdiction. In 2024, we submitted testimony to the Senate Special Committee on Aging outlining needed reforms—including expedited payment reversals and expanded data-sharing with federal law enforcement. We strongly supported bipartisan legislation such as the **TRAPS Act**, which would empower financial institutions to freeze suspicious transfers and work more seamlessly with regulators and agencies to protect seniors and vulnerable consumers.

## 4. Veterans Helping Veterans

What makes defense credit unions unique is not just their customer base—it’s their workforce. Many of our fraud prevention staff and member service specialists are veterans or military spouses themselves. They recognize when something feels “off” and understand how to engage with older veterans who may be too proud or ashamed to admit they’ve been targeted. This trust is the first line of defense.

## Recommendations and Offers of Partnership

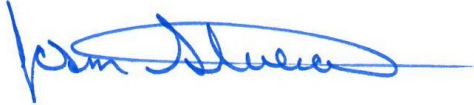
Given the nature of the threats identified in your hearing—and the real-world experience of our institutions—we respectfully offer to:

- **Partner with the Judiciary Committee to pilot fraud prevention programs** within defense communities that could scale nationally. These include AI-based scam detection, real-time alert networks, and joint messaging campaigns with federal agencies.
- **Collaborate on legislative frameworks** similar to the TRAPS Act that expand liability protections for institutions acting in good faith to stop or reverse suspected fraud.
- **Provide expert testimony or briefings** from our member fraud units and compliance teams who work daily to protect older Americans from cross-border scams.
- **Support outreach and education campaigns** targeted at older veterans and military families, leveraging our trusted access on bases and within VA networks.

## Conclusion

As criminals become more sophisticated and transnational in scope, it is imperative that our national response match that scale. DCUC and our member institutions are on the front lines of this fight. We thank the Committee for elevating this issue and offer our expertise and partnership in developing strong, bipartisan solutions to protect those who served our country—and who now deserve our protection.

Sincerely,



Jason Stverak  
Chief Advocacy Officer  
DCUC

CC: Members of the Senate Judiciary Committee  
Members of the Senate Banking, Housing and Urban Affairs Committee

# LOVESAIID

post@lovesaid.org  
www.lovesaid.org



## The Science of Being Scammed: Why Romance Fraud Is More Than a Scam

### Introduction: Not Just a Scam—A Psychological Ambush

Romance fraud isn't a simple case of deception. It's a carefully engineered emotional ambush that uses the most intimate part of us, our capacity for love, as a weapon against us. It doesn't happen because victims are weak or foolish. It happens because they are **human**, with histories, vulnerabilities, and hearts that hoped.

This is not about gullibility. It's about trust. And if you think you couldn't be a victim, ask yourself: *Have you ever loved someone who didn't deserve it? Stayed longer than you should have? Wanted to believe someone could change?* Then you already understand how it happens. This report talks about biology, psychology, trauma, and criminal strategy; and ends by naming the institutions that make it all possible: tech platforms and banks that look the other way.

### The Chemistry of Vulnerability: How Your Body Can Betray You

Imagine this: you're grieving a loss, lonely or isolated, lost a job, moving house, emotionally raw, known as a 'hot state', your body is already working against you. Then someone arrives in your inbox or on a dating app and says all the right things. The chemicals in your body, already amplifying fear, love, hope, make us seek relief, love and validation. With this new character, your brain, already in distress, floods with more chemical that *feel* like connection:

- **Dopamine** gives you a rush every time they message.
- **Oxytocin** makes you feel bonded after a vulnerable conversation.
- **Cortisol** rises when they disappear and hooks you deeper.
- **Serotonin** drops, leaving you anxious, focused only on them.

This is **not fantasy. It's neuroscience.** And it makes it almost impossible to walk away, because your brain and body are already convinced this is real and love.

### Society Trains Us to Trust—Until It's Turned Against Us

From the moment we're born, we're taught to trust those around us:

- That pilots are sober.
- That food isn't poisoned.
- That teachers want what's best for us.
- That romantic partners mean what they say.

This conditioning keeps us sane but it also makes us vulnerable. Scammers *don't need to work hard to build trust.* They only need to imitate the signals we're already trained to respond to. And once those signals are triggered, we often comply without question.

## When Biases Blur the Truth

Even when a warning bell rings, our minds override it with a chorus of rationalisation. Here's why:

- **Confirmation Bias:** You find proof that it's love because you *need* it to be.
- **Sunk Cost Fallacy:** You've already given too much to back out now.
- **Optimism Bias:** You believe this won't end the way it did for others.
- **Similarity Bias:** They're just like you—or so they've made you believe.

By the time the logic returns, it's already too late. You're not questioning *them* anymore, you're questioning yourself.

## A Gold Stamp of Manipulation: Grooming to Control

Romance fraud doesn't start with a request for money. It starts with:

- **Grooming:** Slowly, gently, they learn your needs and give you what no one else has.
- **Love Bombing:** Messages at dawn and dusk. Dreams of your shared future. Promises so intoxicating they eclipse reality.
- **Gaslighting:** Making you doubt your gut, your memory, your friends.
- **Trauma Bonding:** Giving just enough love to keep you hooked, and just enough fear to make you stay.
- **Coercive Control**

They're not improvising. They're following a script, a psychological journey that leads you exactly where they want you.

## Not Just Scammers—Abusers by Another Name

The traits romance fraudsters use mirror the traits of **narcissists and psychopaths:**

- Well documented behaviour patterns that work.
- Performative emotions.
- Control masked as love.

These are the same behaviours seen in domestic violence. If you've ever stayed in a toxic relationship, you already understand the fog: the hope, the fear, the guilt, the shame.

In person Romance fraud criminals use these behaviours instinctively, it is who they are. Just like the abusers of domestic violence.

Cyber criminals rely on that fog. They *create* it.

## The Machine Behind the Mask

These aren't just smooth talkers. They are often part of sophisticated crime syndicates, equipped with:

- Fake documents and photos.
- AI-generated video calls and voice messages.
- Cloned banking apps and websites.
- Well-rehearsed scripts for love, loss, and emergency.

They build a believable character tailored to fit *you*. Not because they love you—but because they know how to destroy you most efficiently. Along with this character, is whole cast to back them up, creating a fake reality around the victim, slowly isolating them from those who can see from the outside, what the victim no longer has power to detect.

## The Triple Trauma: What Victims Are Left With

Victims of romance fraud don't just lose money. They lose their sense of self, their trust in others, and often their will to believe in good again.

1. **The Loss of Love** – The most intense relationship of your life, gone.
2. **The Loss of Reality** – The person you loved didn't even exist.
3. **The Financial Loss** – Your future, security, savings—erased.

All of this is layered on top of the trauma that made you vulnerable in the first place. You're left wondering how it happened, how you missed it, why you can't stop loving someone who was never real. And when you try to speak? You're met with silence, blame, or worse, mockery.

## The Enablers: Platforms and Banks

This level of destruction wouldn't be possible without willing facilitators:

### Social Media & Dating Apps

- Fake profiles created daily in their thousands.
- Little to no verification.
- Reports ignored or brushed aside (automatic signal recognition set too high).
- No use of AI technology to remove profiles with the same face.

### Banks & Financial Institutions

- Fraudulent accounts operating without red flags.
- Obvious payments to high fraud risk areas
- Clear difference to normal spending behaviours
- Victim blaming instead of support.
- No standard protocol for romance fraud response.

These companies profit from traffic and transactions, regardless of whether they come from love or lies. Their inaction is not passive. It's profitable.

## Final Words: Until Systems Change, Victims Will Keep Bleeding

Romance fraud is not embarrassing. It's **orchestrated abuse**. It uses technology, psychology, and systemic negligence to steal not just money—but meaning, trust, and identity. If we don't force platforms to act... If we don't hold banks accountable... If we don't teach people how this works...

Then survivors will continue to suffer silently, wondering how they lost everything to a person who never existed.

You don't need to imagine being scammed. Just remember the last time you loved someone who hurt you. Now imagine they never existed at all.

Statement for the Record

U.S. Senate Judiciary Committee

Hearing: “Scammers Exposed: Protecting Older Americans from  
Transnational Crime Networks”

June 17, 2025  
Washington, DC

Ken Westbrook, Founder and CEO, Stop Scams Alliance  
[www.StopScamsAlliance.org](http://www.StopScamsAlliance.org)



Dear Senator Grassley, Ranking Member Durbin, and Members of the Committee:

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 citizens and financial institutions. The United States must move rapidly to increase our defenses against foreign criminals—especially Chinese cybercriminals—who are using increasingly sophisticated cyber-based techniques to scam Americans at unprecedented scale.

All witnesses at the Committee’s 17 June 2025 hearing agreed that we need a nationally-coordinated response. This Statement for the Record outlines what the response should entail.

Our response should start by recognizing the origin of the threat. Chairman Grassley was correct to open the June hearing by saying “Transnational Organized Crime groups are targeting all of us with industrial-scale fraud.” The United States is under attack by foreign organized crime.

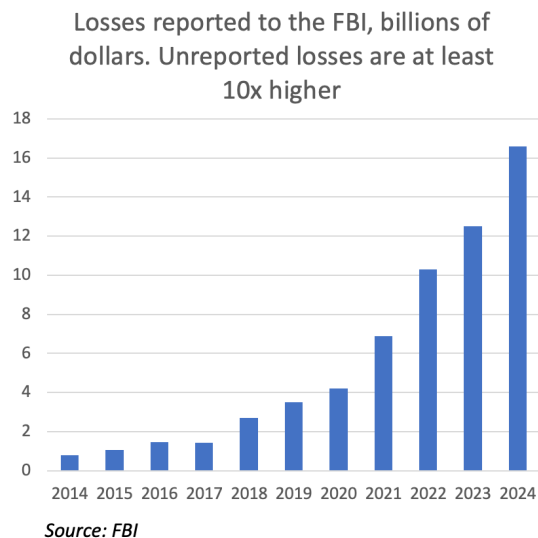
According to FBI, UN, and Interpol reports, the main perpetrators of scams are Chinese crime syndicates located in Southeast Asia: Myanmar, Cambodia, Laos, and other countries. Recently, the criminals have expanded beyond Southeast Asia: the [Center for Strategic and International Studies](#) reports 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 in recent months? [Chinese cybercriminals](#). Cyber criminals who focus on consumer scams are also hosted by such countries as India, Nigeria, Ivory Coast, North Korea, and others.

A recent [Federal Trade Commission report](#) estimates that *total* U.S. fraud losses (reported and unreported) are approximately \$158 billion annually. Losses at this level would exceed the annual revenue of such corporations as Verizon, AT&T, or Bank of America. It would also exceed the annual budget of the Department of Homeland Security.

According to a [poll conducted by Gallup](#) and inspired by the nonprofit [Stop Scams Alliance](#), eight percent of U.S. adults—roughly 21 million Americans—were scammed in the past year. That’s roughly the population of Florida or New York State. In other words, more than 57,000 people are being scammed each day in the United States.

- Gallup found that scams are Americans’ second-highest crime concern (after the related crime of identity theft), with 57 percent saying they frequently or occasionally worry about it.
- Scams are among the [most common crimes affecting Americans](#), according to Gallup.

The growth rate of scams is skyrocketing. According to FBI data, there has been a 20-fold increase in losses reported to the FBI since 2014; reported losses ballooned 33 percent between 2023 and 2024 alone.



U.S. law enforcement is overwhelmed by the tsunami of fraud. A Secret Service official recently [testified](#) that “transnational fraud threats far exceed the current capacity of U.S. law enforcement to sufficiently deter.”

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 terrorism. As criminals increasingly adopt artificial intelligence to make their scams more realistic, the future looks grim.

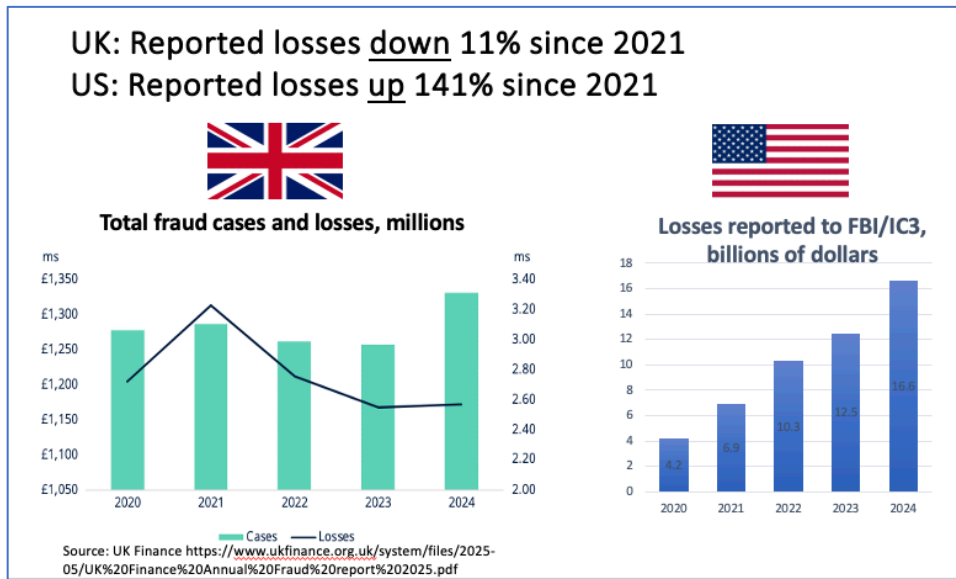
Scams and fraud perpetrated by foreign crime gangs are a threat to our nation’s security. Google declared in a February 2025 [report](#) that the rising surge of financial cybercrime is a “multifaceted national security threat.” [Microsoft](#) also has called the threat environment “increasingly dangerous” and called for government action, saying: “We have to find a way to stem the tide of this malicious cyber activity.” A [Secret Service](#) executive testified last year at a House of Representatives hearing:

*Defeating this organized criminal activity is not just a humanitarian imperative, but a **critical national security concern**, as we have seen substantial interplay between these sorts of organized transnational fraud schemes and foreign efforts to evade sanctions, steal funds, profit from ransomware, and other criminal activity.*

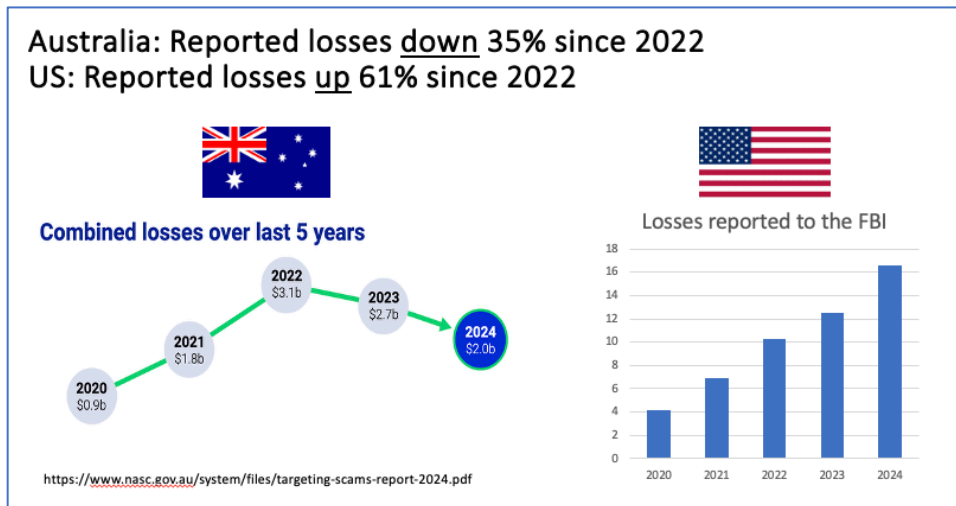
### **It is possible to bend the curve**

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 have declined since](#)

2021, according to the British trade organization UK Finance. This contrasts with the increasing losses reported by Americans to the FBI over the same period.



Australia has also seen 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 US to the FBI over the same period.



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

- A comprehensive national strategy.
- Someone in charge of implementing the strategy (the Home Secretary in the UK, the Assistant Treasurer and Minister for Financial Services in Australia).
- Mechanisms for enhanced public-private partnership.

- Annual government surveys to measure the extent of fraud.
- Centralized fraud reporting.
- A national capability to quickly take down fraudulent investment websites.
- Measures to block fraudulent investment advertisements.
- Measures to block spoofed phone calls and text messages.
- Nationwide education campaigns.
- 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.

To date, the U.S. approach to fighting scams has focused heavily on educating the populace and law enforcement action to seize funds and arrest the perpetrators. All experts agree that these approaches are important and need to be bolstered, but they are not sufficient to deal with the increased threat environment.

The UK and Australia have recently added important elements to the strategy:

- Focus on national leadership, strategy, and public-private cooperation.
- Focus on information collection and data fusion.
- Focus on using authentication and blocking to interfere with the main paths used by scam attacks (digital advertising, malicious websites, spoofed phone calls and text messages).

### **Recommendations for Congressional Consideration**

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

1. Create the proper organization and authorities to defend the nation more effectively from attacks by foreign cyber 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.

We should:

#### 1. Create a national strategy to combat consumer fraud

Congress should declare that fighting foreign cyber scams is a national priority and prioritize the creation of a national anti-scam strategy, as a matter of financial stability and national security. The strategy should clarify authorities about who is in charge in the US Government, create a national-level task force, and include enhanced public-private partnership involving the technology, telecommunications, and financial sectors. The strategy should set goals and measure progress.

We currently have no strategy, according to an April 2025 [report](#) from the Government Accountability Office, which found that “There is no government-wide estimate of the money lost to scams, no common definition of scams, and no national strategy for combating them.”

A. Create a national-level task force. Scams are complex and the response requires close coordination between the private sector and a number of US agencies. We need a national task force that includes a holistic, across-the-government approach combined with public-private cooperation.

In June 2025, Senators Crapo and Warner introduced a bill that represents a step in the right direction, although it is narrower in scope than the national, whole-of-government approach that was articulated in report language in the 2024 Financial Services and General Government Appropriations Bill.

- The Crapo/Warner bill, called the [Taskforce for Recognizing and Averting Payment Scams \(TRAPS\) Act](#) (S. 2019), would direct the Treasury to establish a task force to evaluate methods for preventing scams and issue recommendations for Federal legislation. The purpose and composition of the task force focuses mainly on payment scams and the financial sector. For example, the bill would designate four representatives from financial institutions, but only a single representative to represent “an industry association representing technology or online platforms.”
- In contrast, the 2024 Financial Services and General Government Appropriations Bill is broader in scope, appropriate for addressing the breadth of the scam problem facing the country. It directs 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. ([Financial Services and General Government Appropriations Bill, 2024, S.Rpt. 118-61, July 13, 2023, Cong-Sess:118-1](#))

Since scams begin far upstream from the financial institutions, a national-level task force should include representation from the entire scam ecosystem, including big tech and social media platforms, advertising, and telecommunications providers. Also, 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).

And we must remember that scams are just one attack method used by Transnational Organized Crime (TOC), which also engages in fentanyl production/distribution as well as human trafficking. Consequently, we should think big and create a National Counter TOC Center. 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.

B. Improved Executive Branch coordination. We must be able to answer the question: “Who is in charge of US fraud policy in the executive branch?” As a model, the Judiciary Committee can look to [The Anti-Drug Abuse Act of 1988](#). The Committee played a key role in creating this Act, which 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. Centralization of effort has helped to streamline and

strengthen the government’s response to drug-related issues; focus and centralization could do the same for the fraud crisis facing the United States.

C. Improved 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. Congress could also authorize a **Federal Advisory Committee** to create a whole-of-government strategy with goals and metrics, drawing on expertise from both the public and private sector experts.

D. Create a formal mechanism for enhanced public-private partnership. 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.

If London and Canberra can partner with social media, advertisers, telecoms, financial institutions, and others to fight scams, so can the United States.

## 2. Centralize reporting and enhance information sharing

Centralization and information sharing across government and the private sector would help us identify the threats and respond. Nine nations around the world now have national anti-scam centers—why not the United States?

A. 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.

- The Senate Judiciary Committee played a central role in the creation of the 1984 law that established NCMEC—the Missing Children’s Assistance Act. ([Public Law 98-473](#)). This 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 serves as a hub for information sharing, training for law enforcement, and education of US citizens.
- A similar private, nonprofit organization dedicated to scam prevention could help the United States defend its citizens and financial institutions from attack by foreign cybercriminals.

Financial institutions should be able 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 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, amounts, etc.

- 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 for a known perpetrator. The threshold for unknown perpetrators is \$25,000.
- 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.

Similarly, a **Federal Reserve-backed working group** [recommended](#) in 2024 that the US 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.

B. New legislation should allow safe-harbor sharing of fraud-related information at scale across industries, including the tech, social media, and telecommunications sectors. (For example, The PATRIOT Act Section 314(b) currently applies only to financial institutions.)

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

A. Congress should direct the **Census Bureau** to add scams to the biannual National Crime Victimization Survey so we can 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 fraud survey conducted by the **Justice Department / Bureau of Justice Statistics (BJS)** was in 2017. Congress should provide the funds for annual fraud surveys, which is how the UK and Australia collect the appropriate data to craft their anti-scam strategies.

B. The **Government Accountability Office (GAO)** should combine the siloed information on scams collected by the US government and create the first-ever national estimate of consumer fraud losses. (GAO recently released a [report](#) that estimates the amount of fraud losses to the US 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 the rapid growth in cyber crime that targets consumers and financial institutions. The report should address the identity, locations, and strength of foreign cyber criminals, 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 cyber crime.

#### 4. Create a national capability to quickly take down fraudulent investment websites

Centralized data collection would allow the US to quickly take down fake investment websites, which has proven to be a very effective way to reduce fraud losses due to investment scams. The US Government currently takes down some malicious websites, but our process is cumbersome and ad hoc. Meanwhile,

- The Australian Securities and Investment Commission (ASIC) has coordinated the removal of more than more than 10,000 investment scam websites and online advertisements since July 2023. The result: [Investment scam losses decreased by 35 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](#).
- In the UK, most website takedowns are done by the National Cyber Security Centre, an arm of GCHQ (equivalent to our National Security Agency). UK organizations and citizens send 20,000 reports a day of suspicious emails and URLs. The result: 235,000 malicious URLs have been removed since April 2020. Malicious URLs are removed in less than 6 hours on average, and [the median uptime for a cryptocurrency scam website is one hour](#), according to NCSC. As a result, the number of cryptocurrency scam websites found by the UK government has decreased dramatically since 2021.

## UK: Taking Down Cryptocurrency Scams

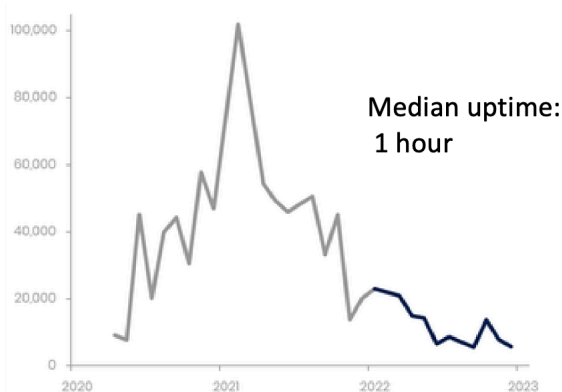


Figure 1: Number of takedowns against cryptocurrency investment scams  
<https://www.ncsc.gov.uk/files/ACD6-full-report.pdf>

## 5. Reduce fake advertising via improved authentication procedures

Criminals use fake advertising to entice victims to engage in fraudulent investments. The US 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. Why aren't these services available in the US?

- 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](#), including, 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 (including [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.”

## 6. Block scam phone calls and text messages

Since most scammers are foreign-based, scams would be reduced if Americans knew when they received a foreign phone call. Foreign criminals often try to gain trust by pretending to be US companies in a telephone call. 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](#).

A. Congress should direct the **Federal Communications Commission** (FCC) to recommend enhanced ways to reduce the ability of criminals—especially foreign criminals—to impersonate legitimate US companies or agencies.

- For example, 19 countries block inbound international phone calls that spoof domestic numbers. (Example: A call from India that pretends to be calling from Los Angeles.) Because most scams emanate from foreign criminals, this measure has achieved significant results.
- Countries that block international calls that spoof a domestic number: [UK](#), [Australia](#), [Sweden](#), [Finland](#), [Norway](#), [Germany](#), [Belgium](#), [Latvia](#), [Lithuania](#), [Oman](#), [Saudi Arabia](#), [India](#), [Singapore](#), [Taiwan](#), [Spain](#), [Czech Republic](#), [Ireland](#), [Poland](#), [Malta](#).

Three countries—UK, Australia, and Singapore—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. In December 2025, to prevent abuse of text messaging systems, [Australia](#) will additionally require the senders of bulk text messages to register.

These or similar authentication measures must be used in the US to restore trust in our telecommunications, which are increasingly being hijacked by foreign criminals. 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.

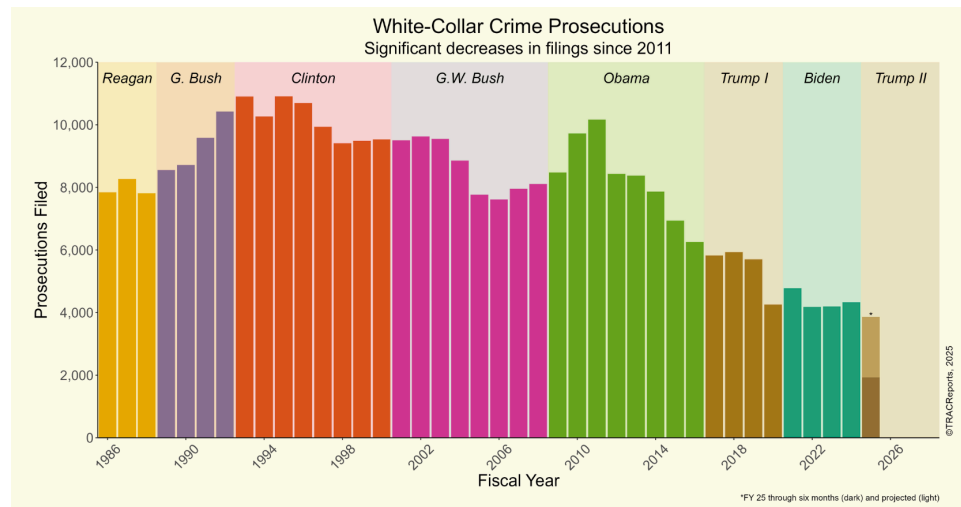
- In addition, the penalties in the 2009 Act have eroded with inflation, so they should be increased to deter scammers who pretend they are representing reputable companies.

## 7. Boost law enforcement resources and intelligence priorities

US 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 is adding 400 new investigators and ordering their intelligence community to “relentlessly pursue fraudsters wherever they are in the world.”

In the US, because of resource constraints, less than 1/10<sup>th</sup> of one percent of fraud cases are investigated, according to a [testimony provided to the Senate Committee on Aging](#). The [FBI](#) initiated 3,020 attempts to freeze funds for victims in 2024. That is less than 1/10<sup>th</sup> of one percent of the total number of complaints (4.2 million).

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 “tech support scam” often begins with a “pop-up”—usually caused by a malicious ad—that takes over a person’s computer. Criminals pose as technology support representatives and often gain remote access to victims’ devices with software that persists for the life of computer, which enables revictimization.

Measured by the number of victims, the “tech support 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.

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. The scam begins with malicious software that can be detected or blocked. The plan should also include recommendations for reducing the risk imposed by remote access software that can be installed with or without a person’s knowledge and runs without warnings—forever.

**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 US economy.**

Thank you for the opportunity to submit this statement for the record. I look forward to working with the Committee on these important issues.

Respectfully submitted,

Ken Westbrook, Founder and CEO, Stop Scams Alliance

[www.StopScamsAlliance.org](http://www.StopScamsAlliance.org)



**America's  
Credit Unions**

**Jim Nussle**  
President & CEO  
202-508-6745  
jnussle@americascreditunions.org

99 M Street SE  
Suite 300  
Washington, DC 20003

June 16, 2025

The Honorable Chuck Grassley  
Chairman  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

The Honorable Dick Durbin  
Ranking Member  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

**Re: Tomorrow's Hearing: "Scammers Exposed: Protecting Older Americans from Transnational Crime Networks"**

Dear Chairman Grassley and Ranking Member Durbin:

On behalf of America's Credit Unions, I am writing regarding the Committee's hearing entitled, "Scammers Exposed: Protecting Older Americans from Transnational Crime Networks." America's Credit Unions is the voice of consumers' best option for financial services: credit unions. We advocate for policies that allow the industry to effectively meet the needs of their over 142 million members nationwide.

We thank you for holding this important hearing on how to combat efforts targeting older Americans. Credit unions were pleased to champion the Senior Safe Act and appreciate its passage in 2018, making it easier for credit union employees to step in and protect seniors facing financial exploitation. Many credit unions have instituted financial education and literacy programs aimed at older Americans and their families to help educate them about methods of fraud and how to detect scams. At America's Credit Unions, we have started our own fraud task force to gather insight from our member credit unions on how to best protect their members. These are just some of the ways that credit unions, as member-owned institutions, work to protect their members.

Credit unions also invest significantly in both security and compliance management systems to prevent unauthorized electronic fund transfers (EFTs) and support faster, innovative payment options for their members. The credit union industry's commitment to relationship banking also gives members confidence that if they have a problem, they can count on their credit union to make every effort to resolve the issue. This emphasis on high touch service means that members will often seek and receive the help of their credit union even when a transaction primarily implicates the services of a third party with which the credit union has no formal, direct relationship. Member interaction with such services, particularly nonbank payment platforms, can complicate error resolution procedures, place strains on a credit union's compliance resources, and magnify exposure to fraud. The costs borne by credit unions stemming from payments-related fraud are growing exponentially and cannot be sustained without limit. Expanding the liability for financial institutions for payments-related fraud, as some have

June 16, 2025

Page 2 of 2

previously proposed, would put a major strain on credit union resources and their ability to collaborate with payments platforms and expand consumer choice.

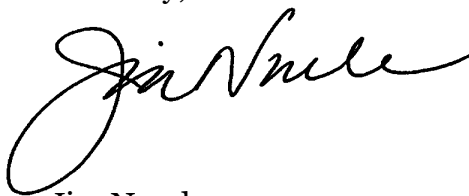
We are, however, pleased to see the recent introduction of S. 2019, the TRAPS Act, to create a task force by bringing together financial regulators with law enforcement and others to study and make policy recommendations to help fight the proliferation of payment scams. We would urge support and action on this legislation.

Finally, we must also flag our concerns with efforts to advance the Credit Card Competition Act because of the impact it would have on the industry's efforts to fight fraud. Proponents of this bill say that it targets large banks and will not hurt others. They are wrong. The reality is that it will hurt community financial institutions and consumers, and we strongly oppose this legislation. This bill would require financial institutions to allow credit card transactions to be routed via an alternative network. Additionally, the bill contains an explicit requirement that card issuers enable all types of transactions and security protocols, even if a credit union finds that these methods are unnecessary, unaffordable, or unsecure. Each time a network is added or changed to keep up with merchant demands, hundreds of millions of new cards would have to be issued which would expose consumers to identity fraud through mail theft and increase the cost of the payments system.

Any reduction in interchange fees from this legislation would directly affect credit union investment in fraud management systems and processes that are dedicated to reducing fraud risk in the system—forcing credit unions to increase costs to cover these necessary expenses. This would limit the consumers' choice when it comes to credit cards and would allow big box retailers to pick which network will process transactions—resulting in the cheapest and least secure networks handling consumers' personal financial information. Critical consumer protections such as fraud protection could disappear by using these third party, less secure networks.

In conclusion, America's Credit Unions appreciates the Committee's focus on protecting seniors from scams and fraud. We stand ready to work with you. Credit unions are committed to fighting fraud, educating seniors, and sharing information necessary to prevent financial crime. We thank you for the opportunity to share our thoughts on this important topic.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim Nussle", written in a cursive style.

Jim Nussle

cc: Members of the Committee on the Judiciary



# Scammers Exposed: Protecting Older Americans from Transnational Crime Networks

Statement of Record

U.S. Senate Committee on the Judiciary

June 17, 2025

The Community Bankers Association of Illinois (“CBAI”) proudly represents nearly 250 community banks in urban, suburban and rural communities throughout the state of Illinois. CBAI appreciates the opportunity to provide our observations and recommendations contained in this *statement of record* for today’s hearing: “Scammers Exposed: Protecting Older Americans from Transnational Crime Networks.” This hearing is particularly appropriate because June is Elder Abuse Awareness Month, which is an annual reminder to protect vulnerable senior members of our communities from exploitation.

Fraud and scams are rampant and on the rise. Particularly insidious are those financial crimes that target senior citizens potentially robbing them of their life savings. Preventing and deterring these crimes is a shared responsibility that includes banks, banking regulators, government agencies, religious institutions, advocacy groups, community organizations, family members, law enforcement and the judicial system. We are pleased to report that Illinois community banks recognize their responsibility and have responded to help combat this pernicious problem.

## **The Scope of Elder Fraud and Scams**

CBAI is disturbed by the shocking numbers concerning elder fraud. According to the FBI, in 2023, and in the United States, there were 101,068 complaints, the total financial losses were

CBAI is dedicated to exclusively representing the interests of Illinois community banks and thrifts through effective advocacy, outstanding education, and high-quality products. CBAI’s members hold more than \$80 billion in assets, operate 940 locations statewide, and lend to consumers, small businesses, and agriculture. For more information, please visit [www.cbai.com](http://www.cbai.com).

approximately \$3.4 billion, with an average dollar loss per incident of \$33,915, and 5,920 complaints reportedly lost more than \$100,000.

These numbers likely underreport the problem because many seniors are embarrassed and less likely to admit they have been a victim of fraud or scams.

### **The Intersection of Vulnerability and Sophistication**

Seniors are primarily concerned, decent and trusting individuals. However, too many seniors are socially isolated; some suffer from a disability, and many have lost a spouse and are lonely. Most seniors are *sharp as a tack*, but unfortunately, some have a degree of impairment, and together with their more trusting nature make them particularly vulnerable targets for fraud and scams.

Fraudsters and scammers are tech-savvy and have knowledge about communications, technology and banking. Generative artificial intelligence gives these criminals the ability to leverage that technology (and potentially link it with the use of cryptocurrency and crypto ATMs) to construct and execute their deception more effectively. This combination of vulnerability and sophistication is the reason elder fraud and scams are not only rampant, but escalating, and becoming more difficult to prevent.

### **Detection and Prevention**

Community bankers are well positioned to assist in the detection and prevention of senior financial exploitation because they are likely to have more in-depth knowledge about the seniors' financial position and habits so that when they see something out of the ordinary, they are in a good situation to question, intervene and stop potential fraud or scams. Community bankers are rightly viewed as highly credible and trusted individuals, so discussions between seniors and their bankers about financial affairs are in the normal course of banking business.

The five federal banking regulatory agencies, the Financial Crimes Enforcement Network, and the state financial regulators have issued a joint statement to provide financial institutions with examples of risk management and other practices that may be effective in combatting senior financial exploitation.

Community banks are encouraged to assist their senior customers in the following ways.

1. Educate their staff and senior customers about fraud and scams.
2. Develop policies and practices to protect senior account holders and their bank.
3. Explore account types (joint accounts for example) and options to review transactions in a timely manner to facilitate fraud prevention.

4. Communicate and cooperate as much as possible with other parties responsible for the detection and prevention of elder fraud and scams.

### **Illinois Requirements**

The state of Illinois has a regulatory requirement, and banks are examined for compliance by the Illinois Department of Financial and Professional Regulation, for mandatory training on elder fraud for new employees and on an ongoing basis. CBAI's Education Department is an approved training provider.

### **Recommendations**

Speed in the execution of fraud or scams is the enemy of effective detection and prevention. Fraudsters and scammers instill a sense of urgency in their intended victims in hopes of defeating any sense of caution that seniors may have. Yet, unfortunately, the victim is often convinced of the legitimacy of fraud or scam. They are coached by the criminals to keep the transaction from being revealed (for instance saying there is a "gag order" requiring non-disclosure, or how to answer banker's questions). Many times, the victim is so insistent on the bank completing the transaction (withdrawing cash or wire transferring funds) that the victim will not cooperate with attempts to stop the transaction. In those instances, it is necessary for senior customers to be responsible for the instructions they give the bank. And tragically, there are times when the perpetrator of the fraud is a relative or friend of the senior citizen and not a faceless criminal.

Community banks are subject to strict laws and regulations to ensure the privacy of the customers' financial information. Bankers that may want to reach out to a family member or other trusted individual are precluded from doing so. Also, the law is not always clear as to whom community banks should report suspected senior fraud and scams and ultimately how the information is being used to successfully deter these crimes.

CBAI surveyed its members earlier this year about fraud and asked:

1. Should banks be allowed to place a temporary hold on an account or deposit items while fraud is being investigated?
2. Should banks be given an indemnity for good faith efforts to protect their customers from suspected fraud and scams?

CBAI members responded unanimously "Yes" to both these questions.

With this unanimous confirmation in mind, CBAI recommends laws and regulations be

implemented to allow community banks to be in a better position to help their senior customers from becoming victims of fraud or scams.

1. Allow community banks to place holds on accounts when they believe a loss from fraud or scams is imminent, including an indemnity for holding those funds.
2. Allow community banks to contact trusted adults who are not listed on the account in the event of suspected fraud or scams. Also, allow community banks to not notify someone listed on the account if they believe the person on the account is complicit in the fraud. There needs to be an indemnification for contacting (or not contacting) individuals regarding fraud or scams.
3. Create a centralized repository for elder fraud and scam complaints, effectively distribute this information to the appropriate branches of law enforcement, promptly react to fraud and scams by the appropriate branch(s) of law enforcement and swiftly prosecute the criminals.

CBAI appreciates the opportunity to provide this *statement of record* to U.S. Senate Committee on the Judiciary at today's hearing. If you have any questions or require any additional information, please contact David Schroeder, senior vice president, federal governmental relations, at (847) 909-8341 or [davids@cba.com](mailto:davids@cba.com).

###

# The Providence Journal

## CRIME

# 'I acted every day in greed': He scammed widows, including RI woman. Now he is going to prison.



**[Katie Mulvaney](#)**

Providence Journal

Updated Oct. 8, 2024, 6:58 p.m. ET

PROVIDENCE – He preyed on the losses of their husbands, their Christian faith, their loneliness and, above all, their inclination to trust.

“You took advantage of goodness,” said U.S. District Chief Judge John J. McConnell Jr. in sentencing [Wisdom Onyobeno](#) to serve 121 months in prison for a sweeping [romance scam](#) that left women, most in their 60s and 70s, in financial tatters, ashamed and reeling emotionally.

McConnell spoke of disbelief that Onyobeno, 44, of Atlanta, continued to perpetrate his crimes and victimize vulnerable senior citizens even after his alleged [co-conspirators were arrested](#).

“I’ve got to assure that you never do this again,” McConnell said. In addition, McConnell said, he must send a message to others inclined to carry out romance scams at a cost of millions in lost retirement benefits and people’s sense of self-assurance and pride.

## Romance scam victims, including former RI woman, share their stories

But first, McConnell heard from victims, including a woman whose financial losses forced her to leave Rhode Island.

“I have been permanently changed. ... Dating is no longer a viable option,” said Beverly Hawes, a 71-year-old widow living in Florida who had been married to her husband for 49 years before he died.

“Four months after I had begun what I thought was a romantic relationship (including an engagement ring, very cheap), the relationship was over and I was out of \$324,650,” she said.

She had to sell a home in Oregon and a motor home, both at a loss, leaving her finances in shambles, she said. To pay off her maxed-out credit cards, she refinanced her home. She's had problems with the IRS and Social Security, and now is in the path of [Hurricane Milton](#).

“I am basically living hand to mouth each month,” she said, adding “Please pray for me.”

“I know the Lord is going to watch over me,” Hawes said after McConnell urged her to take refuge from the storm.

Another woman in North Carolina, who was still without power after [Hurricane Helene](#), told of her mother dying in 2021 after being victimized by Onyobeno and others.

“I’m mentally exhausted and ready for my mom to rest in peace,” she said. She called for Onyobeno’s deportation back to Nigeria.

“He came to this country to scam and take advantage of vulnerable people,” she said.

## **Onyobeno cast as 'unrepentant con man' in romance scam scheme**

In asking that Onyobeno be sentenced to more than 10 years behind bars, Assistant U.S. Attorney Denise Barton cast him as an “unrepentant con man” who played a leading role in a romance scam and money-laundering conspiracy involving co-

conspirators from across the United States and overseas, including in Nigeria. The scheme targeted and bilked elderly widows and divorcees in Rhode Island and elsewhere of some \$5.8 million.

Michael J. Lepizzera Jr., Onyobeno's lawyer, asked for leniency, citing his clean record, college education and time he has served since his arrest in Georgia in 2019. Lepizzera portrayed other co-conspirators as ringleaders.

"There is no doubt about it. They are victims in the truest sense," Lepizzera said of the speakers who addressed the court via video.

Onyobeno pleaded guilty in April 2023 to charges of conspiracy to commit wire fraud and money laundering, and wire fraud; in exchange, several charges were dismissed. McConnell ordered him to undergo mental health treatment.

### **Onyobeno: 'I have no excuse for what I've done'**

Authorities allege that Onyobeno and others falsely claimed to be military members stationed abroad and in need of money to send their belongings home or to travel back to the United States. In other cases, prosecutors said they claimed to be stuck on oil rigs in the Gulf of Mexico.

The women were instructed to mail checks, money orders or cashier's checks to post office boxes or to wire money to bank accounts managed by co-conspirators, including Onyobeno himself.

Often, Onyobeno and others convinced the women to send more money, alleging unexpected and urgent circumstances. Other times, they would pose as government officials and tell victims that additional money was needed to deliver parcels that had been sent from overseas, authorities said.

Once the money was transmitted, the group was alleged to have laundered the funds to disguise their origin. Onyobeno and others created business entities and bank accounts into which they would deposit the victims' money, only to withdraw

it. Sums were sent to Nigeria or used to purchase vehicles that were then sent abroad.

Onyobeno begged the victims for forgiveness, saying he reads and rereads their accounts.

“I have no excuse for what I’ve done. ... I acted every day in greed,” he said.

A co-defendant, Dominique Golden, [is currently serving a 78-month sentence in federal prison.](#)