

**SCAMMERS EXPOSED: PROTECTING OLDER
AMERICANS FROM
TRANSNATIONAL CRIME NETWORKS**

HEARING
BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

JUNE 17, 2025

Serial No. J-119-23

Printed for the use of the Committee on the Judiciary



www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON THE JUDICIARY

CHARLES E. GRASSLEY, Iowa, *Chairman*

LINDSEY O. GRAHAM, South Carolina	RICHARD J. DURBIN, Illinois,
JOHN CORNYN, Texas	<i>Ranking Member</i>
MICHAEL S. LEE, Utah	SHELDON WHITEHOUSE, Rhode Island
TED CRUZ, Texas	AMY KLOBUCHAR, Minnesota
JOSH HAWLEY, Missouri	CHRISTOPHER A. COONS, Delaware
THOM TILLIS, North Carolina	RICHARD BLUMENTHAL, Connecticut
JOHN KENNEDY, Louisiana	MAZIE HIRONO, Hawaii
MARSHA BLACKBURN, Tennessee	CORY A. BOOKER, New Jersey
ERIC SCHMITT, Missouri	ALEX PADILLA, California
KATIE BOYD BRITT, Alabama	PETER WELCH, Vermont
ASHLEY MOODY, Florida	ADAM B. SCHIFF, California

KOLAN DAVIS, *Chief Counsel and Staff Director*

JOE ZOGBY, *Democratic Chief Counsel and Staff Director*

CONTENTS

OPENING STATEMENTS

	Page
Grassley, Hon. Charles E.	1
Durbin, Hon. Richard J.	2

WITNESSES

Bercu, Joshua M.	7
Prepared statement	23
Responses to written questions	45
Finta, Brady	9
Prepared statement	28
Responses to written questions	47
Gunther, Jilenne	6
Prepared statement	30
Responses to written questions	50
Helm, April	5
Prepared statement	42
Responses to written questions	52

APPENDIX

Items submitted for the record	55
-------------------------------------	----

SCAMMERS EXPOSED: PROTECTING OLDER AMERICANS FROM TRANSNATIONAL CRIME NETWORKS

TUESDAY, JUNE 17, 2025

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:37 a.m., in Room 226, Dirksen Senate Office Building, Hon. Charles E. Grassley, Chairman of the Committee, presiding.

Present: Senators Grassley [presiding], Blackburn, Moody, Durbin, Whitehouse, Klobuchar, and Hirono.

OPENING STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Chairman GRASSLEY. Good morning, everybody. We are here today because the scam threat is real. We are all potential victims. The perpetrators are getting more bold, more ruthless, and more global by the day. Transnational organized crime groups are targeting all of us with industrial-scale fraud. These aren't small-time lone wolf crooks. They are sophisticated criminal networks operating with precision across the borders. They exploit technology, including artificial technology, and are draining billions of dollars from Americans' households.

The Federal Trade Commission estimates that scammers stole \$158 billion from Americans in 2023. Almost \$62 billion of that was stolen from our senior citizens. Sixty-two billion dollars would fund the entire Department of Justice for a year and a half. It would fund all public university tuition for U.S. undergraduates for a year, so we are talking about a lot of money.

So where is it going? Transnational crime networks are using American dollars for drug trafficking, human trafficking, arms trafficking, and other evil projects along that line. According to a 2023 Gallup poll, scams are Americans' second highest crime concern just after fear of identity theft. Nearly half of Americans say that they have encountered a cyber attack or a digital scam attempt. Eight percent of U.S. adults, that is 21 million Americans, were scammed in the past year. That means more than 57,000 Americans are being scammed each day.

Scammers are extremely convincing, and their tactics are very effective. Calls from foreign countries appear on cell phones at the local bank branch number, the local police department, or another trusted entity. Artificial intelligence needs just 17 words of a per-

son's real voice to create an entire script that sounds like that individual. So it is believable, then, when a caller that sounds just like your child or grandchild claims to need a few thousand dollars after an at-fault car accident or for some other reason.

There is a scam out there designed to entrap each of us. Americans are pressured, coerced, coaxed, encouraged, or even romanced into emptying their savings, draining their retirement, and wiring funds to accounts controlled by criminal organizations in other countries.

Crime groups in Nigeria are known for internet scams, and crime groups in India are known for tech support scams. Chinese gangs run scam centers in Southeast Asia where trafficked individuals are often forced to carry out scam efforts. Those scams affect all Americans.

We focus this hearing on older Americans for a few reasons. First, older folks are suffering over a third of all scam losses. They often have accumulated more wealth than younger Americans, so they have more to lose.

Second, seniors belong to a generation that is more likely to answer the phone and is more likely to experience loneliness and isolation directly related to age.

Lastly, financial exploitation increases the risk of both physical and mental health issues, particularly for older people. People who have been scammed often experience shame, anxiety, depression, and post-traumatic stress. They also have an increased risk of suicidal thoughts and actions.

This isn't just a call to protect the elderly. It is a call to defend our country's integrity, its financial security, and a moral obligation to protect the innocent.

Before I call on Senator Durbin, we are going to have a 2-minute video demonstrating what we all know is going on.

Proceed with the video, please.

[Video is shown.]

Chairman GRASSLEY. Senator Durbin.

**OPENING STATEMENT OF HON. RICHARD J. DURBIN,
A U.S. SENATOR FROM THE STATE OF ILLINOIS**

Senator DURBIN. Thanks, Mr. Chairman.

I want to apologize initially for being late for the hearing. We had a bipartisan briefing this morning that Senators Thune and Schumer sponsored to discuss the horrific assassination of elected officials in Minnesota over the weekend, and also the experience of a Member of this Subcommittee, Senator Padilla, in Los Angeles last Friday. It was a sobering presentation on the question of the assassination and the vulnerability of many people in public life today. I would say that it calls for action, and this Committee is going to be at the heart of it. We are responsible for oversight for the Department of Justice, Department of Homeland Security, and I believe that we will be called on to consider legislation on this subject in a very timely fashion, so that is the reason I was late. It certainly is no disrespect for the important topic we are discussing.

The amount of fraud perpetrated against older Americans is overwhelming. According to the FBI, people age 60 and older re-

ported \$4.9 billion—that is billion—stolen through fraud with an average loss of \$83,000 last year, up 43 percent from the previous year. Elder fraud is a growing threat, and it frequently goes unreported, as the Chairman said because of the victim's fear, embarrassment, or lack of resources. New technologies like cryptocurrency ATMs pose a heightened risk for older Americans. We are considering a cryptocurrency regulation bill on the floor today. We may even vote on it today. Many of us had amendments that we wanted to offer. Unfortunately, no amendments will be allowed by any Member of the Senate, no amendments. My amendment was to regulate the safety of crypto ATMs.

What are crypto ATMs? They are machines you may find in a grocery store or a shop where you do business, and it looks like you can buy a Bitcoin, and that is all there is to it. There is much more to the story. Crypto ATMs look like a regular ATM you find in gas stations, grocery stores. The big difference is that instead of depositing money with your bank, a crypto ATM allows customers to purchase cryptocurrency, something called a Bitcoin.

These crypto ATMs have become a favorite tool of scammers because once a victim purchases crypto and transfers it to a criminal's digital wallet, it is virtually impossible to trace or recover.

These scammers might be using new technology, but they are following a very old playbook. They call their victim and pretend to be from the victim's bank, or they impersonate a government official. They may announce to the victim that they missed jury duty, and because of it, they have to pay a fine, and to avoid a trial and a fine, they go to a Bitcoin machine and deposit thousands of dollars. Sounds impossible, happens all the time. They may say the victim owes money for skipping jury duty or needs to bail a loved one out of jail.

It happened to my wife. She got a call from our grandson, and she was supposed to send money quickly because he had been in an auto accident. She called me and said, what do you think I should do? And I said, let me ask our grandson, who is standing next to me, whether he was in an auto accident, and the answer, obviously, was no, it was a scam.

They tell their victims all they need to do to make the problem go away is to pay a fine or a fee using the nearest crypto ATM. The scammer walks them through every step. Put in your money, buy your crypto, send it to the scammer's wallet.

Crypto ATM scams led to nearly \$247 million in losses in 2024, 31 percent increase over the previous year. And make no mistake, the crypto ATM companies know that their machines are involved in this fraud. One crypto ATM operator, Bitcoin Depot, wrote in an SEC filing, "Our products and services may be exploited to facilitate illegal activity such as fraud, money laundering, gambling, tax evasion, and scams." That is a stunning admission in their own corporate product.

But it gets worse. I don't want this to be personal, but I want the Chairman to know it. An investigation by Iowa's own attorney general found over 98 percent of the money that the people in Iowa reported sending through Bitcoin Depot was part of scam transactions, 98 percent. Can you imagine? Crypto ATMs aren't being

exploited. They are being used as indicated and misused, obviously, over and over again.

And cryptocurrency in general are also increasingly used for fraud. In 2024, the FBI reported crypto-related crimes up 66 percent. Americans lost \$9.3 billion to crypto scammers, nearly 150,000 complaints filed involving crypto fraud, including more than 6,000 complaints in my own home State, and more than a third of all crypto fraud complaints filed by Americans over the age of 50.

Statistics alone can't paint a complete picture. In Illinois, an elderly woman with MS lost \$40,000, her entire life savings. The woman could not get around very well. The scammer even called an Uber car to pick her up and drive her to the local crypto ATM. This heart-wrenching story and many more like it are the reason I introduced the Crypto ATM Fraud Prevention Act with Senators Blumenthal, Reed, and Welch. It would require crypto ATM operators to register with financial regulators, warn customers about scams, and create transaction limits so that customers won't lose their life savings. The bill also would require operators to refund new customers who have been defrauded.

We have got to do more to protect the people who send us here to do this job, particularly vulnerable older Americans. For God's sake, they paid their dues, they went to work, they saved up meager savings and maybe have a little Social Security on the side, and they barely get by. To be ripped off by one of these frauds has got to be beyond embarrassing. It could be completely destructive of their lifestyle. I stand ready to work with Senator Grassley and my colleagues to address this issue.

Thank you, Mr. Chairman.

Chairman GRASSLEY. Yes, thank you very much.

Now, I would like to introduce our witnesses.

Ms. April Helm, the daughter of a romance scam victim and a founding board member of a nonprofit called Advocating Against Romance Scammers. Following her mother's tragic death, Ms. Helm has dedicated her life to spreading awareness about romance scams and helping those victims. She is also host to a podcast called Scammer Stories, where she has interviewed over 100 people from all walks of life who have experienced scams.

Ms. Jilenne Gunther, the national director of AARP's BankSafe Initiative, a comprehensive intervention platform that equips the financial services industry to prevent and stop financial exploitation of older adults. In her work, she engages frontline employees at banks, credit unions, investment firms, retailers, and other providers of financial products and services. Under her guidance, AARP's BankSafe Initiative has trained 1 in 10 financial industry frontline employees who have saved older adults more than \$100 million from exploitation. Ms. Gunther holds a JD degree from University of Utah, master's degree in social work from Washington University in St. Louis.

After Ms. Gunther, we have Joshua Bercu, the executive director of the Industry Traceback Group and vice president of policy and advocacy at USTelecom, the broadband association. Through the Traceback Group, Mr. Bercu leads an effort to identify the source and stop illegal calls in his USTelecom role. He heads USTelecom's

policy development and advocacy on digital trust and consumer protection. Before joining USTelecom, Mr. Bercu was a partner at the D.C. Telecommunications Law firm's privacy practice where he worked on automatic calling-related legal, regulatory, and policy issues.

Brady Finta, founder and CEO of the National Elder Fraud Coordination Center where Mr. Finta served in the FBI for almost 25 years where his work focused on combating organized crime, gangs, and child pornography. He also served as supervisor of the Cross-Border Violence Task Force where he specialized in transnational organized crime investigations including kidnappings, murders, cartel finance, and money laundering. In 2018, he established the FBI's San Diego Elder Justice Task Force and this year he opened and leads the National Elder Fraud Coordination Center. The center combats scams by aggregating and analyzing private and public sector through an organized crime lens. It ties cases together and creates high-dollar investigative packages of Federal law enforcement investigation.

Now, before you begin your testimony, we swear members at this hearing, so please rise so I can give the oath.

[Witnesses are sworn in.]

Chairman GRASSLEY. They have all answered positively.

Ms. Helm, start out.

**STATEMENT OF APRIL HELM, HOST, SCAMMER STORIES
PODCAST, BOARD MEMBER, ADVOCATING AGAINST RO-
MANCE SCAMMERS, TULSA, OKLAHOMA**

Ms. HELM. Thank you, Senator Grassley and Senator Durbin, for the opportunity to speak with you today. My name is April Helm. I'm here because my mother, Sherri Tyson, lost \$350,000 to a romance scam before her passing in 2020 while undergoing treatment for late-stage ovarian cancer. It's been a long, frustrating, and heartbreaking journey that has brought me to this moment.

And before I share the details, I want to express just how surreal it is that I am sitting here with you today. In 2018, while undergoing cancer treatment, she became even more isolated, more susceptible. One day, while I was headed to a football game in my hometown, I received a text from her. It said, "I gave all my money away, I have nothing, come get me." I was in shock. She promised, but she had lost her apartment, her car, everything. I told her she could move in with me, but on one condition, and that was she couldn't talk to the scammer in my house. She refused. She couldn't let go of the fantasy they'd sold her.

Instead, she moved in with her sister in Mobile, Alabama. And when that didn't work out, she asked me to come get her so she could start fresh in Dallas with my brother. We made a plan to move her that day, but scammers had another plan. One of their tactics is to keep victims awake all night, exhausted, and disoriented. That morning, as my aunt and my mother were preparing to leave, my aunt, who's sitting behind me today, found her collapsed on the floor. She never made it to Dallas. I believe with all of my heart that if it weren't for the scam, I would have seen my mother that day.

In the early days, there was almost no information online about these scams. As someone with a background in radio news, I launched a podcast to investigate, to talk with other victims, law enforcement, and experts. I've interviewed people of all ages and professions who were deceived, smart people. A former CIA agent, she lost \$1 million, a son of a marriage counselor who lost money, a woman who was married to a retired colonel.

This crime isn't just happening to the elderly. It is happening to people my age and younger. A woman my age in Oklahoma recently made national news because her scam turned her into a money mule, like many do, and she is now facing up to 62 years in prison.

I've interviewed the scammers themselves too. One told me they like to target Americans because we have money and because of what we did with slavery.

Many victims go to local authorities only to be told there's no crime because they gave their money away. Victims feel abandoned, penniless, ashamed, and taxed heavily for withdrawing their retirement savings. Some even take their own lives under the weight of the despair.

Today, I serve on the board of Advocating Against Romance Scammers, a national nonprofit focused on prevention, education, and advocacy. My mother deserved better. Every victim does. We urgently need Congress to act to ensure no more families are shattered by this cruel and complex crime.

Thank you for your time, and thank you for listening to my mother's story.

[The prepared statement of Ms. Helm appears as a submission for the record.]

Chairman GRASSLEY. Thank you very much, Ms. Helm.

[Off mic.]

**STATEMENT OF JILENNE GUNTHER, NATIONAL DIRECTOR,
AARP BANKSAFE INITIATIVE, AARP, NEW YORK, NEW YORK**

Ms. GUNTHER. Good morning. My name is Jilenne Gunther, and I'm the national director of AARP's BankSafe Initiative. I'm honored to speak with you today on behalf of more than 100 million Americans aged 50 and older. I have spent my career working to prevent fraud, starting in a prosecutor's office, then at the State level in Utah, and now nationally at AARP.

Congress' work addressing fraud has really opened up opportunities for prevention, from providing immunity for reporting fraud when financial institutions train their staff, to encouraging the sharing of industry-promising practices, and we are seeing the results.

AARP's BankSafe program builds on the goals of those laws. We partner with 1,500 financial institutions to stop exploitation before the money leaves the account. The free training we created with the industry, paired with policy adoption, has helped prevent more than \$450 million from ever being stolen from consumers.

But this fight is personal. It's in my DNA. My grandfather was a banker and a victim. In his 90's, someone was taking cash from his wallet. My uncle, also a banker, noticed the red flags, and in a move only a banker would think of, he planted a dye pack in my

grandfather's wallet. Our family literally caught the thief red-handed.

Most families aren't that lucky. They don't have bankers, and they don't have dye packs. So that is why I built a program at the very bank where my grandfather worked so other families wouldn't have to rely on luck to protect the people they love because fraud isn't an accident. It's a crime. And it's happening at a devastating scale. The FTC reports older adults lose between \$7 billion and \$62 billion a year. In a blink of an eye, someone can lose their entire retirement savings.

The financial industry can be the last line of defense, but only if we give them the authority to act. Let me tell you a story about Brittany. She is a young college student working as a bank teller. After taking AARP's training, she noticed a man acting strangely. He wanted to withdraw all of his money from his account, and he kept on going outside to take calls. She slowed things down, asked the right questions, and she said to me, I wouldn't have caught it without the BankSafe training. Her actions protected this man's life savings of \$50,000. And this isn't rare. A study found that Bank Safe-trained staff saved 16 times more money than those without the BankSafe training.

But we are still leaving tools on the table. Today, most financial institutions can't delay a suspicious transaction unless their State specifically allows it. Yet, according to the American Bankers Association, 90 percent of institutions in those States say holds would be beneficial. A study also confirmed that delaying and holding transactions like the one that Brittany used are among the most effective frontline tools. But there are outdated regulations that really tie the hands of the very people best positioned to act in real time.

Meanwhile, criminals are coordinating across telecom, tech, social media, and the financial industry, while we ask these same sectors to work in silos. We need a Federal coordinated response under your leadership to make this happen. That means empowering financial institutions to delay suspicious transactions without fear of liability, enabling the real-time information-sharing of fraud and requiring social media tech and telecom platforms to become part of the solution, not hiding places for criminals.

Australia is already doing this, and it is working. Scam losses dropped 43 percent after they launched a national response. And this isn't just about stopping theft. It is about protecting trust, preventing negative impacts to business and government, and ensuring the independence of adults in the final years of their life.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Gunther appears as a submission for the record.]

Chairman GRASSLEY.

[Off mic.]

STATEMENT OF JOSHUA M. BERCU, EXECUTIVE DIRECTOR, INDUSTRY TRACEBACK GROUP, SENIOR VICE PRESIDENT, USTELECOM, WASHINGTON, D.C.

Mr. BERCU. Chairman Grassley, Ranking Member Durbin, Members of the Committee, thank you for the opportunity to testify

today and for your leadership on this critical issue. Your continued partnership is vital to sustaining the vigilance, innovation, and coordination we need to fight the scammers exploiting the American people.

I'm Josh Bercu, executive director of the Industry Traceback Group, or ITG, the FCC-designated entity to traceback unlawful robocalls, and senior vice president at USTelecom. I have also served on the Aspen Institute's Task Force for Fraud and Scam Prevention and the FTC's Scams Against Older Adults Advisory Group.

The communications industry has been making meaningful progress confronting scam robocalls. We've deployed tools like call blocking and labeling, stir/shaken call authentication, and traceback. We are leveraging these tools in the fight against ever more personalized fraud schemes. Traceback helps us identify the actors behind fraud calls and has supported dozens of civil and criminal enforcement actions at every level of government. We know the combination of identifying bad actors responsible, including through traceback, and then holding them accountable works.

A couple stats here. Raids of Indian call centers in 2016 led to an overnight 85 percent drop in IRS scam robocalls. And a similar Canada-India crackdown in 2018 led to a 77 percent decline in similar calls to Canadians.

Today, thanks to coordinated action by industry and government, many of the most disruptive, high-volume scam calls no longer reach vulnerable Americans at the same scale. Indeed, scam robocalls are down over 50 percent from their 2021 peak. But today's fraudsters aren't blasting millions of robocalls impersonating the IRS or Social Security Administration. They are targeting individuals with live calls and finely tuned deception. They spoof bank numbers and pose as fraud teams. They impersonate loved ones and local officials to steal from their victims. And as we have already heard today, in the case of older adults, they can rip away what their victims spent a whole life building.

We are not powerless against these devastating scams. It used to take law enforcement months to determine who made an illegal call. And now through ITG tracebacks, we often find those criminals within hours or days. That speed and scalability allow us to keep pace with today's fast-moving fraud.

In recent years, we have proactively expanded our work beyond telecom. Our collaborative cross-sector partnerships have broad tracebacks reach and relevance as a tool for disruption. And they could be a difference maker in building actionable criminal cases. While we can't undo what's been done, we can go after the bad guys and prevent further harm.

The threat of foreign actors exploiting U.S. networks is not new, but their tactics are evolving. Increasingly, we trace calls to foreign actors posing as U.S.-based entities, forming shell LLCs, and in some cases, impersonating real companies, all tactics designed to evade scrutiny. Criminal enforcement remains essential to deter these groups that are orchestrating these scams.

Some tactics, like SIM Box, SIM Box is used to route calls from abroad, require actors to be present in the U.S., creating a rare op-

portunity for enforcement. Turning that vulnerability into a point of disruption and deterrence should be a clear priority.

We're responding aggressively, but we cannot make arrests or prosecute the criminals even when we identify them. That's where we need government support. There are three things Congress can do that would make a meaningful difference.

First, establish a national anti-scam strategy with a designated Federal lead or task force. We need a coordinated Federal response, and we need to treat scams as what they are, crimes. Our strategy must prioritize cross-border criminal enforcement.

Second, provide a safe harbor for improved fraud prevention and detection. Emerging partnerships across industry sectors are showing real promise in identifying and disrupting scams. A well-scoped safe harbor could unlock deeper collaboration.

Third, support and scale what works. As scams evolve, we need to double down on tools and partnerships that have shown real results.

While we have made progress, fraud continues to take a toll. We must now focus on turning progress into impact, helping to deter, disrupt, and penalize fraud, ensuring the criminals can't target another victim.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Bercu appears as a submission for the record.]

Chairman GRASSLEY.

[Off mic.]

STATEMENT OF BRADY FINTA, FOUNDER AND CEO, NATIONAL ELDER FRAUD COORDINATION CENTER, OCEANSIDE, CALIFORNIA

Mr. FINTA. Good morning, Senators. There was a time not long ago when Americans felt comfortable answering the phone and talking to strangers. We weren't suspicious of every number we didn't already know and skeptical that every text or email might be an elaborate scheme to steal from us.

Fraud has become ubiquitous in our country. For hundreds of thousands of older Americans every year, it has a life-altering effect, causing them to lose their life savings, damage their mental and physical health, withdraw from society, and even to commit suicide. As the Chairman said, the FTC estimated losses just to our elders at over \$62 billion a year. Some of these losses include both of my parents.

Where does it go? Transnational organized crime groups overseas, some in countries who are our Nation's adversaries. This is a national security threat we as a country are not effectively mitigating. It's most clearly manifest in the annual statistics from both the FBI and FTC that show dramatic increases year after year, particularly among our elders. I'm unaware of any other crime which victimizes a particular demographic of Americans at these levels.

I think it's time to admit that what we're doing is not enough to stop or even slow the progression of this crime. We have to do something more dramatic. I'd like to make some recommendations

on things our government could do to address this enormous problem.

First, we should better leverage America's private sector efforts. Fortunately, many of America's companies already have capable anti-fraud and vulnerable persons programs, and they are highly skilled at using this data to uncover fraud. But these companies have only a small piece of the elder fraud puzzle. And this puzzle among companies is not getting put together on a regular basis. The same is true with law enforcement. Agencies are not sharing information enough, and even different departments in the same agencies aren't sharing enough.

Next, we should build a network of elder justice task forces across America, EJTFs. As a Nation, we have created task forces to combat internet crimes against children, terrorists, drug trafficking, and gangs, but not to counter those criminal organizations victimizing our parents and grandparents at an epidemic level. The power to change this dynamic is within our grasp by creating these task forces and teaming them up with the public sector.

Historically, State and local law enforcement had little or no role in investigating transnational organized elder fraud cases. However, their investigative resources are crucial in the solution to this problem because there is just not enough Federal agents to adequately counter this threat. Combining these resources will allow for more mutually supporting investigations across the country, as well as prosecution of co-conspirators committing State crimes. This would create the capacity to better handle the enormous number of complaints. Linking the work of these EJTFs and some national oversight would make more effective and efficient mitigation.

We should build a support network for these EJTFs. Each one would need the support of a law enforcement coordination center in that region, aggregating and analyzing the elder fraud complaints collected by the various law enforcement agencies in that area and combine them with complaints from Adult Protective Services, IC3, FTC, and the like. These leads can be analyzed, prioritized, and used to initiate substantial investigations. Proof of this concept lies within the San Diego Elder Justice Task Force and the Elder Justice Coordination Center that supports that task force.

Once created, these EJTFs would have the support and the resources of the National Elder Fraud Coordination Center, a clearinghouse designed to aggregate and analyze and elevate the efforts of the private sector. Coupling the EJTFs with this coordination center would give America's companies the ability to contribute at scale to the elder fraud fight and allow for law enforcement to develop bigger, more impactful investigations faster. Building this network would be a massive first step in bending the curve of elder fraud in America, keeping billions in the accounts of older Americans and inside the U.S. economy.

Thank you for your time. I look forward to answering your questions.

[The prepared statement of Mr. Finta appears as a submission for the record.]

Chairman GRASSLEY. I thank each of you for your testimony, and I will start, and then Senator Durbin, and back and forth that way, 5 minutes each.

Mr. Finta, requiring fast and efficient sharing of data and intelligence is very important. What are the biggest breakdowns in information-sharing between Federal, State, and local agencies when it comes to elder investigations? Would a more formalized information-sharing hub or Federal coordinating mandate help track and take down transnational scam networks more effectively? I think you have touched on this already, but this gives you an opportunity to expand.

Mr. FINTA. Absolutely, Senator. I appreciate the question. I believe it's the only way to make an impact on this crime is to have a whole-of-society approach and a coordinated approach to this. I'll give a perfect example. In just San Diego County, 12 different law enforcement agencies all independently siloed, not sharing information on any of these cases. Until we put that together with a coordination center, you didn't realize that victims in Carlsbad and Coronado and El Cajon and Santee and San Diego were all victimized by the same criminal enterprise, not being investigated by any one of those individual departments or Federal agencies.

Unless we do this nationally, I do not think we're going to be able to get ahead of this crime that grows every single year. However, I do believe we do have the assets nationally between our public and private sectors and these efforts. If we put them together, I think we could create real impact.

Chairman GRASSLEY. More time for you with this question. How does the National Elder Fraud Coordination Center make a difference, and what can Congress learn from your efforts?

Mr. FINTA. So National Elder Fraud Coordination Center, we call it NEFC, essentially focuses on pre-existing efforts predominantly in the private sector. I'll give you another example. Amazon does investigations into fraud and vulnerable persons programs. They come up with a certain number of selectors related to the bad guys in their investigations. We take those selectors, and we share them with telecoms, banks, other nonprofits, other different financial institutions, tech companies, and we aggregate the information that they've collected on those same selectors in order to present to law enforcement.

What that does, it gives law enforcement a huge jumpstart in a type of investigation that would normally take months and months and months to get to that point, saving effort and making each case more impactful.

Chairman GRASSLEY. Mr. Bercu, a recent survey sponsored by Google said 53 percent of Americans report receiving at least one scam call per day. What should we be doing as a Nation to regain trust in our telecommunications system and to protect citizens from the growing rates of scam calls?

Mr. BERCU. Thank you, Senator, and thank you, Mr. Chairman. And I think our industry shares that concern. We all want the same thing, calls people want getting through, calls people don't want getting through, and that's what the industry has really been focused on.

I think the way to really focus on that is we really do have to go after the bad guys. We've built a lot of protections in the network. There's been a lot of enforcement against enablers of that, and what we see is that the criminals behind this just keep adapting and finding new pathways, so I think that's really got to be part of the answer, going after the bad guys.

Chairman GRASSLEY. Ms. Gunther, 13 different agencies currently play some role in collecting data about and fighting scams. There is criticism that they operate in silos, and there is a lot of talk lately about the need to centralize data collection about scams. How might it bolster our law enforcement efforts if financial institutions were able to report fraud to a central repository accessible by law enforcement authorities and financial institutions?

Ms. GUNTHER. Thank you for the question, Senator. It's a great point. Right now, we're very siloed. The IC3 with the FBI is collecting data. The FTC's collecting data, and then the Department of Treasury is, and those really need to be aggregated together so that people can report into that and we can understand more and more about what's happening in this area so that we can have better statistics and know what these criminal networks are doing.

And I think one of the biggest barriers to that is really the privacy concerns that they have with financial institutions not being able to share information because of consumer privacy regulations.

Chairman GRASSLEY. Senator Durbin.

Senator DURBIN. Thanks, Mr. Chairman.

I listened to your testimony, and I am glad to hear all of it, and I think we are all on the same page. The one thing that I am surprised is if there was any reference to crypto ATMs, I didn't hear it. I think that is the new device that is being used with great success by the scam artist.

And I would just refer again to my neighboring State of Iowa represented by the Chairman. Their attorney general is on this case looking at crypto ATMs. An investigation by the Iowa Attorney General's Office found over 98 percent of the money Iowans reported sending to Bitcoin Depot were part of a scam transaction, 98 percent. It gets worse. CoinFlip, another one of these operations, 95 percent for fraudulent transactions. These aren't real.

I had a vaping shop in my hometown of Springfield, Illinois. I asked them to finally remove the crypto ATM machine because the owner was so embarrassed by the older people who came in there crying, tearing up, screaming, putting money into a machine believing that they were saving themselves from a criminal prosecution. I mean, it is an outrage.

So Ms. Gunther, you know what I did with my bill because I worked with AARP to do it. Do you support it?

Ms. GUNTHER. Yes, we do support it, and we've seen firsthand at AARP how victims are being funneled to these crypto ATMs by people, a variety of criminals. And what criminals do is they want to go to those transactions because there are no guardrails to these, right? There's no trained staff like you have—

Senator DURBIN. No do-over.

Ms. GUNTHER. Yep, no do-over. There are no consumer warnings, and there's no claw back. And that's why it's so important to have those guardrails. It's the same that we have guardrails in our tra-

ditional financial industry with banks and credit unions. We have seen that with BankSafe, when there's friction in the system, it gives people that pause to think something's wrong. And so by putting those frictions in the system with crypto ATMs, it will help cut down on fraud.

But I think we really can't get to it until we get to the front end of the issue, which is trying to figure out how to cut it off, the communication from the criminals that are using the social media tech and telecom company platforms to communicate with consumers.

Senator DURBIN. What percentage is using a telephone now for these scam transactions?

Ms. GUNTHER. You know, I don't know that specific statistic, but I'm happy to get that for you for our office.

Senator DURBIN. Mr. Bercu, how much?

Mr. BERCU. I don't know for sure either, but, you know, it is something that we're continuing to focus on is when that communication comes through a phone call.

Senator DURBIN. So when I warn senior citizens who are worried about these scams, be very doubtful of that telephone call. You are not going to get the telephone call from the Veterans Administration or the Social Security Administration. They are making it up. It is all phony, and they are trying to get you to do something you shouldn't do.

I can recall getting a call from my bank, and they said, we are just checking a suspicious transaction. By the time of the end of the phone call, it was clear it was a scam. I told the fellow I just wasn't going to follow through, and he had some choice words for me. But is it safe to warn senior citizens to be extremely doubtful and careful when they receive this telephone communication?

Mr. BERCU. I think, unfortunately, the current status of fraud, it is good to have everyone on their toes. I know AARP just launched a new campaign. I can't quote it, but it's "pause and listen," so I think that's really good recommendations. And one thing I always tell people, if it's a bank calling, tell them you're going to hang up and call back the bank's public number, and if they protest, it's not the bank.

Senator DURBIN. That will be the end of the story. So if anybody asks you for a Social Security number over a telephone, what is the answer?

Mr. BERCU. No, thank you.

Senator DURBIN. Never do it. How about passwords to get into your accounts?

Mr. BERCU. That—I would recommend against that as well.

Senator DURBIN. Let me ask you about the crypto issue, Mr. Finta. You seem to be aware of it yourself.

Mr. FINTA. Yes, sir. Yes, Senator, very common in pretty much every transnational elder fraud case now. It's kind of hard to find one without crypto transactions and specifically the ATMs.

Senator DURBIN. I think some 13 States now have put in safeguards by their State law. Because I cannot offer an amendment to the crypto bill, there will be no amendments, I won't even be able to raise this issue on a National basis. We have got to do it once and for all. This is a classic example of an amendment which, when I was here a few years ago, would have been accepted on a

bipartisan basis, trying to establish some safety when it comes to these scam transactions. But we are being allowed by the crypto industry no amendments, none, to this bill. Take it or leave it.

Chairman GRASSLEY. Senator Moody.

Senator MOODY. Thank you, Chairman. And thank you to all our witnesses for being here today.

I am one of the newest Members of the Senate. As you can see, I am sitting at the kids' table down here—

[Laughter.]

Senator MOODY [continuing]. The most junior Member of this Committee, but the most excited because I was a former Federal prosecutor, a judge, the attorney general of the great State of Florida, and now I get the opportunity to take all of that that I have learned and experienced, especially as it relates to seniors and some of the issues we are talking about, and delve in on a nationwide basis.

And I want to thank you because, as I am hearing you, you are coming up with real solutions and recommendations, pointing out challenges in the way we are structured, in the way we share information, the way we might approach this in a more organized, efficient way. And I haven't heard once that the way we can fix this is to throw a ton of money at the situation. In fact, I think I heard multiple times, we have the resources, we are just not using them in the best way.

And so, as I have been here now for almost 5 months, one thing that continues to shock me is that we will sit through these hearings—I believe I have sat on a hearing of similar substance—and going down the line, we need more money, we need more money, if you only give us more money, if you only give us more money. And it seems pretty now obvious how we have ended up as a Nation with \$36 trillion in debt because there is a culture now here in Washington, and I guess it is now expected by everyone to fix a problem, the only way to do that is you just throw endless amounts of cash at it.

And I have found over the course of my career in working with law enforcement and interest groups as to particular law enforcement issues that sometimes it is a leadership issue, or it is a coordination issue, or it is a structure issue. And it might take a lot less money if we fix that problem first, and so, thank you. This is a refreshing morning of people who know what they are talking about, genuinely offering solutions that doesn't just include throwing endless amounts of cash at a situation.

And I want to echo something that Ms. Helm said. This problem spans all walks of life. Smart people are falling for these issues. And I think the specific reason seniors are targeted is because they have life savings, and sometimes they are not as adept or skilled at using rapidly evolving technology, whether that is to safeguard their assets that they're trying to manage online, or whether they are not used to using social media platforms in a way that is safe. So this is a challenge.

As attorney general, I noticed very quickly that our Federal agencies many times have a limit or a loss where they will actually prosecute. And sometimes that could be \$5 million. And while the average person might lose what seems to be a little bit amount to

a Federal agency, when accumulated amongst all the victims, it could in fact exceed that, but we are not sharing information and we don't know what that true loss is.

So in Florida as attorney general, we set out to create the first of its kind in the Nation at a statewide level, working with our individual counties of law enforcement and even then our cities to make sure they knew that there was a State-level resource to share this information, these victims, so we could accumulate that data and go after. And we saw some success right away. You have the skilled people at the statewide level that were able to help their local jurisdictions and law enforcement, and if it met a certain threshold, then start working with the Federal Government when they would take that.

And I will start with you, Mr. Bercu. I think you alluded to this. Do you believe that having a Federal approach or one person in charge of working with States at a statewide level to start developing the expertise and law enforcement acumen as it relates to cyber crime and cyber fraud in seniors is absolutely needed right now because we are seeing more and more of these cases take place and could in fact exceed what would be a Federal cutoff?

Mr. BERCU. Yes, I think absolutely. I think it's right for Federal leadership, for Federal coordination with the States and across the Federal Government too because even with the Federal, the FTC, FBI, FCC, DOJ, they all have a role. And so just that—we need a central coordinator that raises this issue to the level of prioritization it deserves.

Senator MOODY. And I will turn to you, Mr. Finta. You kept referencing the problem here are these silos. There is no information gathering. There is no real organizational structure to have the folks that are dealing with it at a Federal level interfacing with statewide because most States don't have targeted teams like this. What would be your recommendation if one were to approach doing that at a Federal level? Where would you even start?

Mr. FINTA. I would basically start with what we already have. We've figured this problem out to some degree with respect to internet crimes against children where we put ICAC task forces in every major city in the United States, predominantly staffed by State and local officers with a prosecution model, DA's Office, U.S. Attorney's Office working together. These ICACs are able to actually infuse the hundreds of thousands of leads they get every year.

We could duplicate that with EJTFs and actually start to get our hands wrapped around this problem. And the thing that we don't understand or that we're not seeing is because there are so few cases right now, the amalgamation of the intelligence of those few cases will get dramatically heightened when you have more of those cases. So if we just mimicked that model and built these EJTFs, it would start to change things.

Senator MOODY. Thank you, Mr. Chair.

Chairman GRASSLEY. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Mr. Chair. And I want to thank my colleagues for the kind words about the murders that happened in Minnesota and the work that needs to be done going forward. The people we lost were tremendous people.

And so I will start with a question actually out of the U.S. Attorney's Office in Minnesota because they presented the evidence yesterday to the Nation. In 2023—and they are fine people that work there—they successfully prosecuted three people who defrauded over 150,000 elderly victims across the country, stole nearly \$300 million from them by convincing seniors to pay to enroll in fraudulent magazine subscriptions. It was one of the largest elder fraud schemes in our Nation.

Like Senator Moody, my former life as a prosecutor, I actually started an elder white-collar crime division in our county attorney's office and know how bad this can be.

Mr. Finta, what barriers do these government and law enforcement agencies face in seeking information necessary to fight scams, securing information?

Mr. FINTA. Well, unfortunately, I think there's a pervasive thought process, particularly among our local law enforcement agencies that there's nothing we can do. Bad guys are overseas, money is in crypto, it's already gone. There is always something we can do, especially if we just start documenting these cases and working together. There's plenty of people in the United States who are co-conspirators in these criminal enterprises that are necessary for them to operate effectively. Those turn into great leads as soon as they get arrested.

Senator KLOBUCHAR. Right, thank you.

Ms. Gunther, in 2022, Senator Collins and I actually enacted a bill, passed a bill, Senior Fraud Prevention Act, to create an office in the FTC focused on fighting scams that target seniors, education, which some of you have referred to. Quickly, do you agree that investing resources targeted at stopping elder fraud scams is an effective strategy in trying to educate seniors?

Ms. GUNTHER. I definitely think that with educating seniors, it's part of a step that we need to have. We know that it's effective when we're actually educating people, and there's different ways to educate people with behavioral tools so they're actually making changes and can recognize and spot those specific red flags of a scam. So we do think—but there are other tools. We need to give tools to the financial industry to actually stop suspicious transactions because education isn't all—is not a one—it's not a one-size-fits-all. We need to give—we need to have a coordinated Federal response. We need financial institutions to be able to stop—

Senator KLOBUCHAR. So just—

Ms. GUNTHER [continuing]. You know, pause—

Senator KLOBUCHAR. Exactly.

Ms. GUNTHER [continuing]. On those suspicious—

Senator KLOBUCHAR. And then one of the things I am concerned about is just slashing the FTC's Bureau of Consumer Protection budget by 13 percent or effectively dismantling the CFPP, the Consumer Financial Protection Bureau. To me, that seems like a bigger problem, which is what is in the budget right now that we just received from the administration. Could you comment on that?

Ms. GUNTHER. Yes, I can't comment on that, but I can put you in contact with someone from our office.

Senator KLOBUCHAR. Okay. Very good. But I just think we should realize what is going on.

I want to turn quickly to AI. I actually have had in my—someone I know well whose son serves in the Marines. He got a call when his son was deployed that was his son's voice that had been scraped off the internet. This isn't a senior scam, but we are seeing so much of this with seniors. And saying, I am in trouble, I need money, basically. And he figured out something was wrong when he started asking questions and hung up. But I think the grandma might not have done that or the grandpa.

Ms. Helm, you testified about some of the ways scammers have ruined lives. What should people know about the dangers of AI-generated scams?

Ms. HELM. Yes, when my mother went through her scam, this was right before AI exploded, so they used very archaic tools of a video of a man in a dark room, and they would voice over the actor in the video. And they were actually pretty convincing, enough to convince my mom to give \$350,000 away.

But with artificial intelligence, this is going to explode. They are so convincing, and they've got money to back people up to make—to back people up to make these scams even more convincing. They'll send you a \$100,000 check, and it will cash.

Senator KLOBUCHAR. Makes you think we should be doing some rules of the road on AI, which we have had a bipartisan effort going on. And one of my biggest fears of this is just the scams that are going to affect individual people. Senator Blackburn and Senator Coons and Tillis and I have worked on deepfakes, but we have to make sure this incorporates some of these scams going forward with what we do.

Ms. Gunther, do you want to add anything on AI?

Ms. GUNTHER. Yes, so with artificial intelligence, it is very scary. We're seeing them adopted. We're getting calls, hearing from our members where they're cloning voices. It's very difficult to use AI to detect that, and so that's why it's really important to have other tools as well. Not only do banks need to adopt artificial intelligence, but they need to do it at a faster pace. But they also have to use other tools in the bucket as multifactor authentication as well.

Thank you.

Chairman GRASSLEY. Senator Blackburn.

Senator BLACKBURN. Thank you, Mr. Chairman.

And to each of you, thank you for being here.

Ms. Helm, I thank you for weighing in and working with us as we developed the Romance Scam bill that we have been moving forward with at Commerce Committee.

Ms. HELM. Thank you.

Senator BLACKBURN. And I appreciate your input on that. You know, one of the things we realized was the entry point for a lot of these scams and these financial crimes are the dating apps, and especially the dating apps for seniors. And so when you talk about an entry point, that seems to have been it.

But what we have learned, and Mr. Chairman alluded to this in his opening, these are really transnational organizations, and this is a big business. And I know U.S. consumers lost, the estimate is \$1.3 billion last year in these scams. But that is what is reported. And we know many of these don't get reported because of embar-

rassment, or they figured it out, but they have already lost several thousand dollars in the process.

And as we were working on our legislation, what we found is that some of these sophisticated transnational criminal organizations will actually promise people that they will get them to another country, many times the U.S., for high-paying jobs.

But what actually happens is it is a form of human trafficking tied to it. They are brought here, and then they are placed in what are called fraud dens. And in these fraud dens, they work the internet, they work the phones, and they create these relationships, and then they are scamming people out of hundreds of millions of dollars every year and telling these individuals that they were going to bring to the U.S. and people that they are trafficking that they have to work out their debt, so that is how they keep them in these dens.

But Mr. Finta, I want you to speak for a minute about these transnational organizations and what we know about them and their underpinning as it relates to these crimes.

Mr. FINTA. Thank you, Senator. These TOC, transnational organized crime groups, they're not really any different than the Mexican cartels, the, you know, TOC groups doing cyber crimes. They're configured relatively similarly, particularly in the way they launder the money.

So one thing that we noticed doing elder fraud investigations is that a lot of the money that we were tracing through these accounts was also in the same accounts with proceeds from narcotic sales, human trafficking, all kinds of other crimes. So it's not necessarily about the crime as much as the criminal groups.

So we have the sophistication in our government and in our private industry to do these investigations if we coordinate them and work them together to have more effect. I think it's more a function of us choosing how to do that as opposed to letting the crooks choose because they're plenty sophisticated. We need to be at that same level.

Senator BLACKBURN. Yes, and I think—and you alluded to this earlier—as we have worked on the Kids Online Safety Act and worked with industry and worked with parents, we have seen some of this skillset develop, and it could be transferred over.

Mr. Bercu, I want to ask you—and thank you for the work you have done on tracing the illegal phone calls, the robocalls and those things. Talk a little bit about traceback and give me an example of where traceback and/or a cross-sector collaboration has led to a criminal conviction and to unraveling part of this network.

Mr. BERCU. Yes, thank you for the question. I think we would love to see more of our work lead to criminal convictions, and that's where we just really think that needs to be a priority. Where a lot of our work—so we trace the calls, we get examples from illegal calls, referrals from law enforcement, data we source ourselves, working with the financial institutions, tech companies, others, and we'll trace that back to the source. And basically, we see 8 to 10 different voice service providers touch that call along the way, and so that's why we need traceback to find out where it really came from, who made the call. So that's the traceback effort. It's been

very successful in civil enforcement. Where we'd love to see it amped up is in the criminal side.

Senator BLACKBURN. Okay. Let me ask you this. With Wi-Fi calling, have you been able to follow any on Wi-Fi calling? And if someone is using a VPN, does that obstruct your work?

Mr. BERCU. So for us, yes, our focus—if it hits the public telephone network, we trace it back. If it's purely over the top, like a WhatsApp call, that would be outside the scope of what we do.

Senator BLACKBURN. Okay. Thank you, Mr. Chairman.

Chairman GRASSLEY. Senator Whitehouse.

Senator WHITEHOUSE. Thanks very much.

I just want to flag for any Rhode Islanders who might be listening, that if you are getting texts and emails that say you owe a toll and that proceedings are about to begin against you because of unpaid tolls or tickets, consider that to be a scam and be very wary about clicking onto any link in that text that purports to be the way that you are going to pay off the unpaid toll or ticket and know instead that this is almost certainly a scam.

The Department of Motor Vehicles and the Rhode Island Bridge and Turnpike Authority have both put out notices that these are not their way of dealing with customers who owe them money. And so when you see that, be very, very wary. That is my public service announcement for the day.

I would also like to put into the record the story of a Rhode Islander who was the victim of a romance scam and lost a great deal of money to a scammer who was sentenced to serve 121 months in prison by then Chief Judge John Jack McConnell in Rhode Island.

It is hard to overstate what happens to an elderly person who is both betrayed by someone who she thought was a romantic interest, who she thought was a friend who she had come to count on, and then also to come back from that and find that her finances are in complete disarray, and she is going to have to really rethink what the rest of her life looks like, that it is going to change her entire financial position going forward.

So I ask unanimous consent to put that into the record.

Chairman GRASSLEY. Without objection, so ordered.

[The information appears as a submission for the record.]

Senator WHITEHOUSE. One of the things that helps the fraudsters is anonymity that is very often provided by VPNs or by fake names. Very often the big platforms have a role in all of this, and we don't have a whole lot of time right now, but I really would be grateful if each of you, if you have thoughts about what the best things that we could do to penetrate the anonymity where it is a part of a scam and to figure out how to hold the platforms more accountable for supporting these frauds. I would be grateful because I think, you know, this has been a good hearing, Mr. Chairman. It has been very bipartisan. Everybody has constituents who are being scammed by these predatory folks. Some of them are from overseas.

When I was U.S. attorney, we had what they called 419, I think they called them, scams, where like a Nigerian minister suddenly discovered that he had \$4 million squirreled away and just needed to get your account information so he could store it in your account, and you would get \$2 million of the \$4 million, and he would get

the \$2 million. It was going to be a great deal. All you had to do was give him all your bank information. Yes, how did that work out?

So the more we can drill into who is really behind these things, the trick with those is trying to figure out who was at the other end of it. And the Secret Service did a pretty good job of investigating. But now, anonymity is even worse, and therefore, these frauds are practiced more prevalently and with less accountability.

So your thoughts on dealing with the anonymity problem and how we can break through that to find the perpetrators more regularly, I would really be grateful for.

And thank you for the hearing, Chairman. Question for the record, we will call that.

Chairman GRASSLEY. Senator Hirono.

[Off mic.]

Senator HIRONO. Thank you, Mr. Chairman. And I thank all of our witnesses.

Clearly, scamming elders has been going on for way, way too long, and I think they are a particularly vulnerable group of people because perhaps part of it is that, one, they may have resources, but two, they may be trusting. They may be trusting. I remember telling my mom who lived with us that if anyone ever calls to not respond to them and she said, but that is very rude because I told her, you have to just hang up. She said, that is very rude. I said, well, then just say no thank you and hang up. But I think that, you know, the fact that they are very vulnerable is, yes, one wonders what more we can do. I think there is more, of course.

So I think there is bipartisan support for the idea that we should work together to combat this type of targeted fraud, but it is, you know, pretty much all kinds of fraud that has to do with the financial fraud. And the thing is that it bothers me that in February, the CFPB was effectively shut down. And as we know, CFPB educated Americans about scams and responded to complaints, and it returned over \$21 billion from basically financial scams. So this is not a time to be shutting down a very effective agency. And that is probably maybe one of the reasons that it is being shut down.

And then in April, the DOJ announced that it was disbanding its National Cryptocurrency Enforcement Team and would no longer target crypto-mixing services that criminals used to launder the proceeds of their scams. And I led a letter to the DOJ asking for a briefing on this topic, but I received no answer. And we know that there are these crypto ATMs that are very busy scamming money from unsuspecting people, so there is a lot going on.

And hearing from all of you, I was particularly interested in Ms. Gunther saying that—and you represent AARP. Now, that is one group that spends a lot of time informing your members about these kinds of scams. But you mentioned that there is more that the financial industry can do to alert people, could be alerting their relatives, that their parents are being scammed, whatever. And you said that Australia had done something, had enacted legislation to enable financial institutions to put holds on what could be raised red flags. Can you tell us more about what Australia has done?

Ms. GUNTHER. Yes, absolutely. Australia is a great, promising practice. It's been in the last year or two that they've put this to-

gether. They've done kind of what we've all been talking about here today, which is a coordinated national response, but it's also bringing all of the players in the ecosystem, every point of the scam, of the journey of the scam for a consumer, whether that's telecom, social media, the financial industry, tech companies, all together to make them responsible because I think we're looking just at the end point, which is the financial industry.

And to your first part of your question is that the financial industry, their arms are tied because they're not able to, when they tell or seize, hey, this is suspicious, there's a red flag here, they're not able—and that person still wants their money. Because of old regulations, they have to process that in about half of those States. Half the States don't have the ability to hold.

Senator HIRONO. So do the other witnesses agree that this is something we can look at doing, following what Australia is doing to bring a lot of people together? In fact, Mr. Bercu, you said that there should be a nationally coordinated response to these kinds of scams. So would you agree that—would all of you agree that, you know, we need to focus on what is happening to our elders and put together a national response? Would you all agree that that would be a good thing? And it would probably require legislation.

Mr. BERCU. I mean, I can say I agree. I think there's a lot of work the industry is doing. There's little segments of work that's across it, but I think we need a government-led national strategy that's in coordination with the private sector, absolutely.

Mr. FINTA. I couldn't agree more.

Senator HIRONO. Okay. I did have one last question for Ms. Helm. It sounds as though your mother, not only was she scammed by this romance scam, but even when she knew that this was a scam, she still continued to want to participate. So there is a whole psychological aspect to this kind of scam that we need to also address.

Ms. HELM. That's the biggest riddle of this whole thing. I could not get my mother to stop. And all the families I speak to, about 90 percent of them email me or call me and say, how can I get my family member to stop? And that's the answer that I—that keeps me up at night. I don't have an answer. I know we do need more therapists who are aware of the problem. And there is one therapist in particular, Cathy Wilson, out of Littleton, Colorado, who is putting a program together to teach other therapists about the emotional impact of romance scamming.

Senator HIRONO. Thank you. Thank you, Mr. Chairman.

Chairman GRASSLEY [off mic]. This concludes our hearing. I thank all the witnesses for the hard work you put into it and the time you spent to get here to share your personal experience and your expertise, and your perspectives are pretty darn important to everybody that gets hurt by these crimes.

Now, we have a process for written questions. They can be submitted for the record for 1 week from today. And then for you witnesses, for answering these written questions, we would like to have you 2 weeks after you receive them, if you could get them back to us.

Thank you all very much.

[Whereupon, at 11:54 a.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

**Prepared Testimony of Joshua M. Bercu
Executive Director, Industry Traceback Group
Senior Vice President, Policy, USTelecom — The Broadband Association
Before the Senate Judiciary Committee
Hearing on “Scammers Exposed: Protecting Older Americans from Transnational Crime
Networks”**

I. Introduction

Chairman Grassley, Ranking Member Durbin, and Members of the Committee:

Thank you for the opportunity to testify today and for your leadership on this critical issue. Your continued partnership is vital to sustaining the vigilance, innovation, and coordination we need to fight the scammers and fraudsters exploiting the American people we all serve.

I’m Josh Bercu, Executive Director of the Industry Traceback Group, or ITG, and Senior Vice President of Policy at USTelecom — The Broadband Association. For ten years, USTelecom has led the ITG, which serves as the entity designated by the Federal Communications Commission to trace back suspected unlawful robocalls. I also have served in leadership roles on the Aspen Institute FSP’s National Task Force for Fraud & Scam Prevention and the Federal Trade Commission’s Scams Against Older Adults Advisory Committee.

Our industry has been making real and meaningful progress confronting illegal robocalls, including both scam robocalls and illegal telemarketing campaigns. The communications industry has developed and deployed powerful tools and mechanisms like call blocking and labeling, the STIR-SHAKEN call authentication regime, and industry-led traceback – all of which are complemented by a strengthened accountability regime at the FCC and aggressive enforcement by government partners at the federal and state level.

We are leveraging these tools in the fight against ever more persistent and personalized fraud schemes. While not every one of the tools translates directly to stopping all forms of fraud, many have proven highly effective in disrupting the infrastructure that enables transnational scam operations.

From this work, we’ve seen both what’s possible and what’s still urgently needed. Because even with these tools, fraud losses are growing as tactics are evolving. Today’s fraudsters are using automation and deception to launch smarter, more targeted attacks that can do just as much if not more harm.

II. Disrupting Scam Infrastructure Through Traceback and Enforcement

Traceback is one of the tools we have adapted to disrupt call-based scam operations. By rapidly tracing the path of illegal calls back through the network, we help identify the upstream providers and actors enabling or originating fraud. Over the past several years, traceback has

contributed to dozens of enforcement actions – civil and criminal – by federal agencies and state attorneys general. We also have begun to work with international law enforcement partners.

We know the combination of identifying the bad actors responsible, including through traceback, and then holding them accountable works:

- Raids of illegal call centers in India led to an 85% drop in robocalls unlawfully impersonating the IRS in 2016.
- Enforcement targeting those responsible for unsolicited vacation and timeshare robocalls led to those calls dropping by half in 2017.
- A joint effort between Canadian and Indian authorities targeting illegal call centers in India led to a 77% decline in calls impersonating the Canadian Revenue Agency in 2018.
- FTC enforcement led to a 60% decline in unlawful health insurance robocalls in 2019 and FCC and state attorneys general action led to the virtual elimination of the illegal auto warranty robocall campaign between 2021 and 2022.

Today, thanks to coordinated action by industry and government, many of the most disruptive, high-volume scam calls – like those impersonating the IRS or Social Security Administration – no longer reach vulnerable Americans at the same scale. And while scam robocalls remain a concern, data from YouMail shows their volume is about 50% lower than at their March 2021 peak.

But the success in reducing illegal robocalls has overlapped with a deeper shift in the fraud landscape. Even as scam call volumes fall, losses to scams have continued to climb, reaching record highs. These scams, including those that begin outside the voice network, are driving the 25-30% increase in fraud losses over the past year.

Criminals evolve. They've shifted from mass robocalling to more targeted, sophisticated attacks. That evolution makes disruption harder, in turn making traceback and enforcement more essential than ever.

III. Meeting the Fraud Threat: Building Partnerships and Collaboration

Today's fraudsters aren't blasting millions of robocalls impersonating the Social Security Administration. They're shifting from high volume to high impact, targeting individuals with live calls, stolen data, and finely tuned deception. They spoof bank numbers and pose as fraud teams. They script emotional appeals. They impersonate loved ones, local officials, and public safety agencies. And they don't need volume to succeed — they just need to know their target's vulnerabilities. They prey on trust and use it to steal from their victims.

In the case of older adults, they can rip away what their victims spent a whole life building.

The good news: we are not powerless against these deeply personal and devastating scams. Traceback is an essential tool. It used to take law enforcement agencies months to determine who made an illegal call — we now often find those criminals within hours. That speed and scalability allow us to keep pace with today's fast-moving fraud.

In recent years, the ITG expanded its collaborative footprint beyond the telecom industry to voluntarily include banks, major tech companies, the hospitality industry, and more. These partnerships have helped broaden the reach and relevance of traceback as a cross-sector tool for fraud disruption. They also could be a differentiator in building actionable cases for criminal law enforcement against the call source. While we can't undo what's been done, we can go after the bad guys and prevent them from defrauding someone else.

For instance, the ITG is proactively piloting a project with several major banks and carriers to identify when a bank's number has been spoofed, launch tracebacks based on that data, and help identify other potential victims. Early results have been promising, and we believe it can serve as a model for enhanced cross-sector collaboration. Beyond this pilot, individual voice service providers are also forming partnerships across industry sectors to explore ways to strengthen real-time fraud detection, alerting, and response.

International coordination continues to be another essential frontier. The threat of foreign actors exploiting U.S. networks is not new, but their tactics are evolving. Increasingly, we trace calls back to entities posing as U.S.-based providers: forming shell LLCs, using disposable domains, and in some cases impersonating real telecom companies. These tactics are designed to evade other providers' know-your-customer programs and regulatory scrutiny. They reinforce why criminal enforcement remains essential. Civil enforcement alone cannot deter the groups of individuals orchestrating these schemes.

SIMBoxes add another layer of complexity. These locally deployed devices allow scammers to simulate thousands of unique mobile identities. To a carrier, they usually look like thousands of individual callers rather than one high-volume source, making them harder to prevent. But they require someone physically present in the U.S. to operate, which creates a rare opportunity for enforcement. These actors are within reach of domestic law enforcement and turning that vulnerability into a point of disruption and deterrence should be a clear priority.

Meanwhile, AI is further blurring the line between robocalls and live scams. Criminals can now use AI-generated voices that pause, laugh, and respond in real time. These tools are cheap, scalable, and increasingly convincing. While analytics-based call blocking and labeling and call authentication can stop some of this activity, the core challenge remains: a growing volume of targeted, sophisticated attacks that are harder to detect, and often more damaging.

The industry is moving aggressively to respond in the face of these evolving threats. We are evolving our tactics, our tools, and our partnerships. But we cannot make arrests or prosecute the criminals — even when we identify them. The most effective way government can support this

work is to strengthen public-private partnerships, unlock additional cross-sector collaboration, and ensure that criminal actors face real consequences for exploiting Americans.

IV. What Congress Can Do

The reality is this: fraud evolves quickly and regulation moves slowly. We cannot legislate or regulate our way out of every new scam tactic. That's not a sustainable model. What we need is a framework that is nimble, targeted at the actors causing harm, results-focused, and supportive of the tools and partnerships that work.

There are three things Congress can do that would make a meaningful difference.

- **Establish a national anti-scam strategy with a central coordinator and prioritize criminal enforcement.** The United States need a unified, whole-of-government approach that elevates scams as a national policy and enforcement priority. A designated White House federal lead or task force would improve coordination, eliminate silos, and give industry a clear point of contact – accelerating action against rapidly evolving threats.

Critically, the strategy must prioritize cross-border criminal enforcement. The actors we identify in tracebacks of scam calls are not confused marketers. They're criminals, often operating transnationally, who are undeterred by regulatory fines. Strengthening support for prosecution, training, investigations, and cross-border coordination will help ensure these actors face real consequences.

- **Provide a safe harbor for improved fraud prevention and detection.** Emerging partnerships between telecom providers, financial institutions, tech platforms, and other stakeholders are showing real promise in identifying and disrupting scams. A well-scoped safe harbor could unlock even deeper collaboration across the internet ecosystem to accelerate threat detection and to better prevent consumer harm. Right now, however, privacy regulation and other legal concerns can inhibit companies from using and, where appropriate, sharing data that could help identify and stop fraud.
- **Support and scale what works – including proven tools like traceback.** As scams evolve, we need to double down on tools and partnerships that have shown real results. Traceback is one such tool: it can help drive criminal prosecutions, civil enforcement actions, and real-world disruption of scam networks, and increasingly serves as a model of effective cross-sector collaboration. But like many effective solutions, it requires sustained support and legal clarity to remain viable. Congress should reinforce frameworks that work like traceback, ensuring stability for the program and protecting it from litigation designed to undermine the process and the program's mission.

V. Conclusion

While we've made progress – together – fraud continues to take a toll. Scam robocalls are down, enforcement actions are up, and industry tools like traceback are evolving with the threat.

But the progress in reducing illegal call volume doesn't mean the threat is gone. Criminal fraudsters are adapting quickly, targeting individuals, impersonating trusted institutions, and operating from beyond the perceived reach of U.S. enforcement.

Our next phase of work must expand our focus on converting intelligence into impact, using traceback and cross-sector collaboration not just to detect fraud, but to help deter, disrupt, and penalize it, and prevent perpetrators from targeting another victim.

Strengthening the public-private partnership, especially around coordinated criminal enforcement, is one of the most important ways the federal government can help turn progress into real accountability and deliver meaningful protection for the American public.

Thank you for your time, and I look forward to your questions.

Good morning, Senators.

There was a time, not so long ago, when Americans felt comfortable answering the phone and talking to strangers. We weren't suspicious of every number we didn't already know or look at every email and text with skepticism that it may be an elaborate scheme to steal from us.

Fraud has become ubiquitous in our country. For hundreds of thousands of older Americans every year, it has had a life altering effect, causing them to lose their life savings, damage their mental and physical health, to withdraw from society, and even to commit suicide.

According to the FTC, older Americans lose over \$61B a year to fraud. Where does it go? It goes to Transnational Organized Crime groups overseas, including to some in countries who are our nation's adversaries. This is a national security threat that we, as a country, are not effectively mitigating. This is most clearly manifest in the annual statistics from the FBI and FTC that show increases of up to 30% in fraud losses year after year, most significantly from our elders. I am unaware of any other crime which victimizes a particular demographic of Americans at these levels. It's time to admit what we are not doing enough to stop or even slow down the growth of this crime, and that it is time to make dramatic changes. I would like to make some recommendations on things our government can do to address this enormous problem.

Fortunately, many of America's companies already have mature and capable anti-fraud / vulnerable persons programs. These companies are highly capable of using the data they have to uncover fraud and those programs hold small pieces of the overall elder fraud puzzle. Unfortunately, they're generally working independently, and these pieces are not being put together with those of other companies. The same is true with law enforcement. Different agencies, or even different parts of the same agency, are not coordinating intelligence related to fraud to build the most impactful investigations on a regular basis.

As a nation, we have created task forces to combat internet crimes against children, terrorists, drug trafficking organizations and gangs, but not to counter those criminal organizations victimizing our parents and grandparents at an epidemic level. The power to change this dynamic is within our grasp by creating these task forces and teaming them up with the private sector.

Historically, state and local law enforcement have taken little or no role in investigating and prosecuting elder fraud cases. However, the investigative resources of state and local law enforcement are crucial in the solution to the problem, as there are not enough federal agents to adequately counter the threat. Combining resources will allow for more mutually supporting investigations across the country as well as the prosecution of co-conspirators committing state crimes. Deputizing, training, and funding state and local law enforcement to staff Elder Justice Task Forces (EJTFs) will create the capacity to better handle the enormous volume of complaints

related to these crimes. Linking the work of these EJTFs with national oversight will make their work more effective and efficient.

Each of these EJTFs will need the support of a law enforcement coordination center for that region, aggregating and analyzing the elder fraud leads collected by the various law enforcement agencies in that area and combining them with complaints from Adult Protective Services (APS), IC3 and the FTC. These leads can be analyzed, prioritized and used to initiate substantial investigations. The proof of this concept lies within the San Diego Elder Fraud Coordination Center, a joint effort among the 12 law enforcement agencies in San Diego County to understand the true scope of the elder fraud threat in San Diego and to make informed decisions on how to best use the limited resources of the San Diego EJTF.

Once created, these EJTFs will have the support and resources of the National Elder Fraud Coordination Center (NEFCC), a clearinghouse designed to aggregate, analyze and elevate the efforts of the private sector. Coupling the EJTFs with NEFCC will give America's companies the ability to contribute at scale to the elder fraud fight and allow law enforcement to develop bigger, more impactful investigations faster.

Building this network will be a massive step in bending the curve of elder fraud in America, keeping billions in the accounts of older Americans and in the U.S. economy.



Testimony of

Jilene Gunther, JD, MSW
National Director, Bank*Safe* Initiative
AARP

on

Scammers Exposed: Protecting Older Americans from Transnational Crime Networks

before the

U.S. Senate Committee on the Judiciary

June 17, 2025

AARP Point of Contact:
Clark Flynt-Barr
Director of Government Affairs, Financial Security
(cflyntbarr@aarp.org)

My name is Jilene Gunther, and I am the National Director of AARP's BankSafe Initiative. I am honored to be here to testify on behalf of AARP, which advocates for the more than 100 million Americans age 50 and older. I would like to thank you and the members of the Senate Judiciary Committee for holding this important hearing, "Scammers Exposed: Protecting Older Americans from Transnational Crime Networks." AARP has long worked to educate consumers, support financial exploitation victims, and improve financial exploitation detection and prevention across industries, and we look forward to working with you towards policy solutions to prevent exploitation and protect victims.

I've dedicated my career to improving the lives of older adults. I began my career in a prosecutor's office advocating for crime victims and later worked on legal strategies preventing fraud at the state level. Nationally, I've focused on practical and scalable ways to help the financial industry prevent exploitation of older consumers. Overall, my work has been replicated in over 40 states and cited in reports by federal agencies like the CFPB and GAO—so this issue is one I've been working on for decades. Today, I run AARP's business-to-business solutions for issues of financial exploitation, dementia, financial caregiving and accessibility—with a focus on the financial industry as a key player in protecting vulnerable adults. We've worked with 1,500 financial organizations across six financial industry subsectors, and our program has helped save more than \$450 million from being stolen from consumers.

But this fight is not just professional for me—it's built into my DNA.

My grandfather was a teacher, a foster parent, a refugee sponsor, a state legislator—and a banker. When he was in his 90s, we discovered he was being financially exploited. Small amounts of cash over a period were disappearing from his wallet. My uncle, also a banker, recognized the red flags. And in a move only a banker would think of, he planted a dye pack in the wallet. That's how our family caught the thief—literally red-handed.

Most families aren't that lucky. They don't have bankers in their family. They don't have access to dye packs. That experience lit a fire in me. I built a fraud prevention program at the very bank where my grandfather once worked—so other families wouldn't have to rely on luck to protect the people they love.

Financial exploitation is a global crisis with devastating, personal and localized consequences. It strips older adults of their financial security, emotional well-being and independence. Combating this crisis requires a comprehensive, coordinated approach that includes the financial industry, technology platforms, telecom companies, regulators, law enforcement and Congress. We must move beyond viewing exploitation as an unfortunate accident or victim's mistake. It is organized crime, and those affected are victims of theft and deception. Perhaps most terrifying: It can happen to anyone.

Elder Financial Exploitation Data and Impact

Elder financial exploitation (EFE) is the illegal or improper use of an older adult's funds, property or assets—including fraud. While the issue of fraud is not unique to older adults, it often has a disproportionate financial impact on them. According to [FBI data](#), older adults

reported higher losses than younger adults in 2024, with an average loss of \$83,000 for those age 60-plus reporting a fraud loss, compared to \$19,000 for all ages.

Older adults are often targeted by criminals because they have more money – they have had a longer time to accumulate savings and are therefore appealing targets for criminals. These losses can have significant impacts on the financial security of older Americans, as they are often living on fixed incomes and can scarcely afford to lose funds to criminals.

Common methods of exploitation fall into two main categories: crimes perpetrated by strangers and crimes perpetrated by known others, such as family members or caregivers.

Stranger-perpetrated scams often rely on fear, quick actions and irreversible transactions. Some of the most common scams include the perpetrator impersonations and tech support schemes. In other instances, the perpetrator preys on people using dating or social media applications, pretends to be in a relationship with their victim and eventually asks them for money. Caller ID spoofing is a deceptive tactic where scammers falsify the information displayed on your phone's caller ID to appear as a trusted entity, such as a government agency, bank, or even a family member. This manipulation aims to exploit a victim's trust and extract sensitive information or money. And now, we are seeing AI being used to impersonate a loved one's voice and/or write a spoof email.

Perhaps more emotionally devastating is exploitation by someone the victims knows. In these instances, perpetrators take advantage of their long-established relationship with the victim in order to gain direct access to funds, such as through joint account ownership or a power of attorney. These are especially threatening because the perpetrator can make recurring and large withdrawals without the victim knowing, robbing that person of their hard-earned savings. Because of their direct access to the account, these instances can be harder to detect and are woefully underreported.

Both forms of exploitation can be financially devastating. According to FinCEN's [review](#) of the latest Bank Secrecy Act (BSA) report data, scams perpetrated by strangers account for most reported exploitation. The average reported suspicious activity amount for these types of scams was a staggering \$129,483. Still, theft by known others averaged an amount of \$98,863 when reported, underscoring the need to address both types.

Using a first-of-its-kind methodology to measure the annual financial cost of EFE in the U.S., [AARP recently found](#) that victims ages 60 and older lost at least \$28 billion annually factoring in unreported cases – a conservative estimate based on three reputable datasets: the [FTC's Consumer Sentinel Network](#) report, which relies on self-reported data to government and nonprofit agencies; the [FBI's Internet Crimes Complaint Center](#), which consists of consumer reports of cybercrimes; and the [Department of Treasury's EFE SARs data](#), consisting of reports of suspicious activity reported by third parties, such as financial institutions or government agencies.

We are currently updating this study with new datasets, which we hypothesize will show an even larger annual loss among older adults.

The problem with relying on self-reported data is that there are massive rates of underreporting among instances of elder financial exploitation. This may occur because of feelings of shame, embarrassment, fear of retaliation or simply not knowing that a crime has even occurred or how to report it.

Most victims never get their money back, often resulting in permanent financial insecurity. Financial loss is compounded by a reduction in overall well-being, including increased rates of cardiovascular conditions, anxiety, depression, reduced life span and even suicide. Further, the financial consequences are devastating and long-term. Many victims have their life savings stolen, jeopardizing their retirement security, and those on fixed incomes rarely recover. Fraud can decrease older adults' trust in essential relationships and systems. Victims may withdraw from family, community and institutions, making them more vulnerable to repeat instances of exploitation.

From a system perspective, reimbursement and financial recovery is rare, and victims must navigate a confusing and often dismissive system without adequate resources or trauma-informed support. All of these consequences make prevention and victim support that much more important.

Exploitation has costs beyond the victim. The financial sector unsurprisingly [loses billions of dollars every year](#), and a CFPB report indicates that institutional filers of SARs reports lose on average [\\$17,000](#) per case. Family members also incur costs to support their financially strapped relatives, and taxpayers pay for [programs](#) that [support victims in need](#).

AARP Exploitation Prevention Work

AARP's exploitation prevention programs are focused on reaching two core audiences: older adults and the financial industry. The [Fraud Watch Network](#) is AARP's program focused on helping our nation's older adults understand the very real threat to their financial security that fraud represents. For the purpose of this testimony, I will focus on the second audience: the financial industry.

[The BankSafe Initiative](#) is a business-to-business (B2B) solution centered on working with the financial industry to stop financial exploitation before money leaves the account. BankSafe encourages the financial industry to voluntarily adopt proven corporate policies that protect consumers and prevent exploitation. To do that we equip banks, credit unions, investment firms and peer-to-peer payment (P2P) platforms with resources, policy templates, training and tools to prevent financial exploitation of older adults.

BankSafe is built on the belief that protecting consumers doesn't have to come at the expense of business efficiency. Rather than an adversarial approach, we are in favor of practical, collaborative solutions that work for everyone. At our core, we are guided by two principles: meaningful industry collaboration and an unwavering focus on the consumer. Prior to its national launch in 2019, we convened over 20 roundtables and qualitative interviews with policymakers, industry leaders, regulators, non-profits, law enforcement, and consumers to understand the

principles driving industry adoption. We found from qualitative interviews with institutions proactively fighting exploitation simply makes good business sense: it prevents loss, creates stronger customer relationships, increases brand distinction and improves employee morale and performance.

We conducted [research](#) with consumers on their needs and wants from AARP and the financial industry. That process pointed to a specific mandate: stop financial exploitation before the money leaves the account.

To that end, AARP has partnered with over 1,500 financial institutions across six subsectors (banks, credit unions, investment firms, retailers selling gift cards, and the P2P providers) to implement industry-wide safeguards and policies that better protect consumers. BankSafe provides a suite of offerings to help the industry prevent financial exploitation. These most often include:

- **Training.** Among BankSafe's most lauded and prominent tools are its training offerings, designed in close collaboration with the industry to reflect real-life scenarios and the needs of those who regularly interact with consumers. Training frontline employees (those managing potentially suspicious transactions as well as those having personal interaction with consumers) who are often in the best position to identify red flags and stop exploitation, is crucial. Unlike many existing trainings that focus solely on legal compliance and reporting, BankSafe goes a step further by equipping staff with actionable, research-backed strategies to intervene and stop exploitation in the moment. Through such tools as scenario-based videos, BankSafe training includes guidance for spotting red flags, research-backed action steps or what the industry refers to as risk-mitigation steps to intervene in suspicious transactions, and how to spot cognitive decline in consumers.
- **Internal policies and procedures.** BankSafe provides financial institutions and staff with policy templates, guidance to help them delay, hold or refuse suspicious transactions. Included are recommendations for suspicious-incident documentation, escalation procedures, AI-based alerts, and account features for financial caregivers and having trusted contacts on record to alert them of suspected cognitive decline and EFE. I have personally seen the impact of these policy recommendations as part of my recent role on the Federal Trade Commission's (FTC) [Stop Senior Scams Act Advisory Committee](#), where the FTC and AARP encouraged industry leaders to voluntarily adopt BankSafe-modeled policy changes to better protect consumers.
- **Promising Practices.** As part of our work, BankSafe identifies and shares promising practices from around the globe—real strategies financial institutions are using to prevent fraud and exploitation. We engage directly with bank leaders, credit union executives, and frontline staff to understand what is working in practice. Rather than prescribe a one-size-fits-all solution, we highlight peer-driven examples so that each institution can assess and determine what aligns with their goals. In our experience, institutions are more likely to consider and adopt a strategy when it is presented by a peer rather than a nonprofit. It lends credibility and facilitates informed decision-making.

The Role of the Financial Industry

The results of a [study](#) evaluating the BankSafe program clearly show that the financial industry is uniquely positioned, and increasingly prepared, to be the last line of defense against the growing epidemic of financial fraud targeting older Americans.

In 2018, a [Virginia Tech study](#) with over 2,000 frontline employees in 11 states (including Minnesota and Vermont) found that employees who took the BankSafe training saved 16 times more money than those without the training. Based on these findings, we estimate that BankSafe policies, interventions, and procedures have, to-date, prevented more than \$450 million from being stolen from consumers.

Results show that the program significantly improved employees' ability to recognize red flags of exploitation. In fact, financial institution staff who completed the BankSafe training were able to identify suspicious patterns earlier and intervene with four times greater confidence. One top financial institution, which manages millions of consumer accounts, reported suspicious instances twice as often after implementing the BankSafe training.

In [one notable case](#), Hayley, a teller who had just taken the AARP BankSafe training, was able to recognize that an older customer was under pressure to wire money. She told me off-camera that she knew after taking the course that her first customer was going to involve fraud. Sure enough, an older gentleman walked in just like in the BankSafe video that she had watched. She said, "I was so nervous when I started to see the red flags. [The BankSafe training] made me feel confident that this was a financial exploitation...before I had even had to bring our fraud department in." Hayley used skills learned through BankSafe to gently delay the transaction, ask informed questions and work with internal fraud teams to block the transfer and help the customer save nearly \$30,000. A Deputy Chief Risk Officer with a financial institution said that after rolling out AARP resources, their frontline workers are more empowered to spot and address fraud. They tell their department, "Oh, I had this customer in. This was the fraud scenario, but we've resolved it, and I just wanted to report that to you. And I definitely see a level of competence and empowerment of our frontline staff. That's a huge win for our customers and our institution. I credit that to AARP BankSafe."

The financial industry's role is critical not just because of its proximity to financial activity, but also because of the trust and consistency that customers associate with their banking and financial relationships. Bank tellers, call center agents, fraud risk managers, member service representatives, wealth advisors and branch managers often see subtle changes in behavior, such as hesitation, confusion, nervousness or unusual transaction requests, that may be invisible to even close family members. They, as well as BSA officers, operations and security employees, and AI analysts, also notice transactional red flags, such as a change in mailing address, atypical withdrawals, opening a new joint checking account, or payments to a new recipient. These positions help them to notice when something is wrong and take appropriate action, provided they have the training and protocols to do so. As the study shows, without that training, these moments of insight can be lost. With it, they become opportunities to intervene and prevent

irreversible harm. This underscores a critical point. Prevention on the front lines is possible, and it is most effective when systems are designed for early detection and fast, informed intervention.

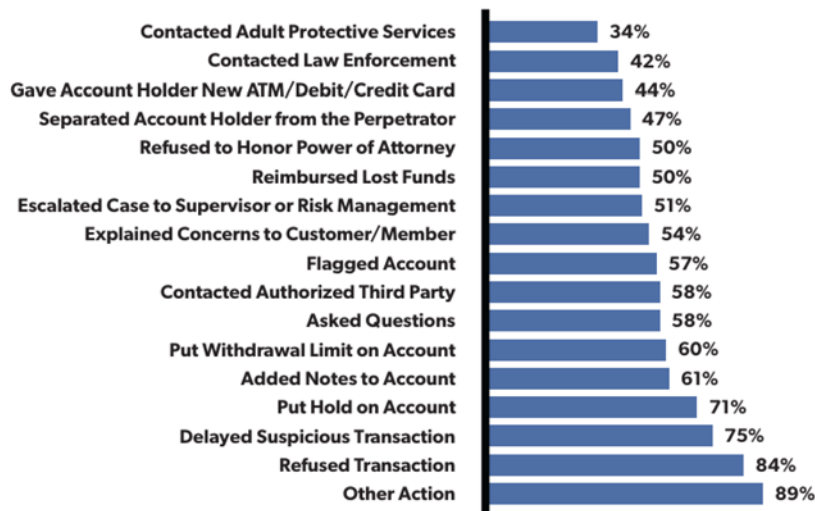
Proven Industry Interventions

There is no one-size-fits-all solution to addressing exploitation. Older adults face a wide range of threats, each requiring different strategies for prevention and response. While the threats are varied, one thing is constant. Financial institutions are uniquely positioned to *spot* and – more importantly – *stop* exploitation before irreparable harm occurs.

The following are proven interventions that demonstrate how targeted, industry-led solutions can better prevent exploitation and protect older adults before money ever leaves the account.

- **Empowering the front lines:** Preventing elder financial exploitation begins where it most often occurs: at the point of transaction. Banks and credit unions that prioritize frontline intervention are seeing real impact. Training tellers, call center representatives and member service staff to recognize and stop exploitation is one of the most effective tools available today. When properly equipped, these professionals are not only able to spot suspicious behavior, but they can stop fraud in its tracks. [We know](#) that in one out of every two interventions by trained frontline staff, financial exploitation is successfully prevented before any money is lost. That makes frontline education a proven safeguard and an essential investment.

CHART 3 - FREQUENCY OF ACTION STEPS INVOLVED IN SUSPECTED INCIDENTS IN WHICH MONEY WAS SAVED FOR ALL PARTICIPANTS



Source: [*The Impact of Training Financial Professionals to Prevent Financial Exploitation*](#)

- **Account protections and networks of support:** Some institutions and fintechs (i.e. EverSafe) are also embracing built-in account features that offer added layers of protection for older customers. “Read Only Access” is a tool that allows a trusted individual to monitor an account without the ability to withdraw funds, creating oversight from a named trusted person without sacrificing autonomy. Similarly, Trusted Contacts allow financial organizations to reach out to a pre-approved individual when something appears amiss. These proactive features empower institutions to act quickly, respectfully and with the consumers’ best interests in mind. As fraud schemes become more emotionally manipulative, having another set of eyes and a trusted advocate can make all the difference. Principles of psychology tells us that someone needs to be told by three different people before they are able to absorb and act on that information. Thus, the financial institution and a trust named person become critical parts of stopping fraud.
- **Leveraging AI, machine learning and technology for proactive protection:** Advancements in AI and predictive analytics can help identify abnormal behavior patterns linked to scams. They even allow consumers to [verify](#) the legitimacy of suspicious texts or emails using databases of known scam, a capability that could become standard in fraud prevention. Monitoring analytics can flag an illegitimately opened account, a warning for potential identity theft. Similarly, predictive analytics can profile customer behaviors to flag deviations, such as irregular Social Security deposits, atypical keyboard typing patterns or predict. [Models suggest](#) that a sudden change in payment behaviors, along with subprime credit scores, can predict dementia more than two years before it is discovered by a physician.
- **Preparing and responding to cognitive decline:** The financial industry also plays a critical role in responding to the complex challenge of cognitive decline. On average, older adults lose [up to half](#) of their median net worth before receiving a dementia diagnosis. The industry can mitigate this loss by recognizing the signs of cognitive decline, responding with empathy and activating support networks like trusted contacts. Institution-level policies, training and readiness protocols are key. To advance this effort, AARP just launched the [BankSafe Dementia Hub](#), a centralized resource to help financial institutions understand cognitive decline and implement actionable solutions for supporting affected consumers.

Challenges Facing the Financial Industry

Despite progress toward implementation of these proven intervention policies, challenges and limitations still limit the industry’s ability to fully protect the nation’s most vulnerable consumers.

- **Inability to Hold Suspicious Transactions:** One of the most pressing challenges is the lack of clear, consistent guidance around reporting and holding suspicious transactions. “Report and hold” laws allow financial institutions to delay or refuse transactions when

they suspect financial exploitation, giving time to intervene before money is irreversibly lost. Research from Virginia Tech has shown that even brief delays can significantly reduce harm, especially when the victim is already in a heightened “fight-or-flight” state and may not be capable of rational decision-making. However, while these laws are effective, especially when used by broker dealers who are federally permitted to act under them, a regulatory gap remains. Banks and credit unions, primary depository institutions, are generally barred from using these tools unless their individual states have explicitly passed laws allowing it. This is due in part to the limitations imposed by federal Regulation CC (enacted in 1989), which governs funds availability and does not provide carve-outs for suspected fraud. As a result, the institutions best positioned to stop real-time exploitation often lack the legal authority to do so, despite clear evidence that the intervention works. In a recent [report](#) from the American Bankers Association nearly 90% of banks located in states that do not have the power to hold suspicious transactions would find it helpful to have that ability.

- **Sharing Information Across the Industry, Telecom and Social Media Companies:** Even when fraud is suspected, privacy laws like the Gramm-Leach-Bliley Act and Regulation P make financial institutions cautious about sharing information, fearing legal liability. As a result, each institution operates in a silo, unable to warn others about ongoing exploitation. These same restrictions limit telecom, social media companies, and the financial industry to sharing information with each other in real-time about these criminal networks. This gap allows scams to continue unchecked, despite clear evidence that coordinated information sharing and intervention could prevent substantial harm. Without federal clarity or safe harbor provisions, institutions that want to protect their customers are left constrained, while criminals remain agile and connected.

Promising Practices and Opportunities to Do Better

These barriers are not insurmountable, but they require coordinated action from policymakers, regulators, law enforcement, telecom companies and the financial industry.

- **A Broader Ecosystem to Fight Fraud:** To truly get ahead of exploitation, we have to look upstream – to the point where the problem begins. Scams don’t start at the financial industry level—they often begin with a text message, a social media post, or a fake ad. That means the first critical moment to intervene isn’t at the teller window or during a wire transfer, but earlier—before the consumer enters the psychological state of panic, fear, or urgency that scammers count on. Once someone is in “fight-or-flight” mode, rational decision-making narrows, making interventions much harder. With the explosive growth of telecommunications and social media over the past two decades, it’s no longer enough to focus prevention solely on banks and credit unions. We need layered defenses across the full scam journey, and that means requiring telecom and social media platforms to act as the first line of defense. Real-time data sharing across sectors—while safeguarding consumer privacy—is essential. Evaluating strong identity verification measures and ad authenticity checks, along with enforcement procedures for removing fraudulent advertisements, to stop fake ads from being launched and widely distributed

across online platforms. Criminals thrive on the fact that these industries often operate in silos, slipping through the cracks.

- **Sharing Information in Real Time:** There's growing momentum for open collaboration and cross-sector data-sharing. The idea is to bring together social media, messaging platforms, advertising networks—even telecommunications—not just banks. By pooling real-time fraud intelligence like suspicious URLs, scam-related phone numbers, and transaction red flags, it becomes possible to detect illicit activity much faster. I recently traveled to the U.K. to speak to industry leaders about this very opportunity. The industry in the UK is in some ways advanced when it comes to regulations and industry-led initiatives to protect vulnerable groups. Successful [pilot programs](#) in the UK, for example, showed that sharing across sectors can surface scam threats a day or more earlier than bank-only systems. And in Australia, programs like Meta's FIRE [initiative](#) with the Australian Financial Crimes Exchange helped eliminate thousands of scam pages early on. To work effectively, this kind of collaboration must include privacy safeguards, support sharing across jurisdictions, and operate near real-time—ideally within 48 hours of identifying a credible risk.
- **Broader Accountability:** Countries like Australia and the UK are leading the way by mandating cross-sector collaboration and holding platforms accountable. In the UK, TSB Bank offers a voluntary [Fraud Refund Guarantee](#), reimbursing every genuine victim of authorized push payment scams—up to £1 million per claim—and has done so since 2019. The bulk of their reimbursements for spoofing scams recently came from a single telecom provider. Unfortunately, the telecom company didn't block the known scam numbers until mandated. This highlights the problem: without banks, telecoms, and platforms working together, we get isolated fixes that don't actually stop the scams. At best, we're patching holes while the system continues to leak. The Australia models show that earlier, coordinated action can stop scams before money ever leaves a consumer's account. In 2023, the Australian government launched the [National Anti-Scam Centre](#), bringing together banks, telecom companies, and digital platforms to coordinate a national response. Under its new [Scams Prevention Framework](#), these industries are required to take preventive action, including removing fraudulent accounts, delaying suspicious transactions, and sharing threat intelligence. A targeted campaign against job scams led to the removal of more than 29,000 fake social media accounts and 1,850 fraudulent job listings. In the final quarter of 2023, reported scam losses dropped by 43% compared to the previous year. These results show that when scams are stopped where they start, real consumer protections follow.

In addition to promoting these fraud prevention policies, AARP is advocating across the country for important consumer protections that will deter criminals from leveraging cryptocurrency kiosks in their schemes. AARP's Fraud Watch Network has seen a dramatic increase in fraud victims being directed to send funds via cryptocurrency kiosk. Improving protections will prevent older Americans from losing hard-earned money to criminals. This includes requiring money transmitter licensing of cryptocurrency ATM operators in the state, implementing daily transaction limits to limit the appeal of these machines to criminals, and refund provisions.

AARP has worked with the North American Securities Administrators' Association on model state legislation to enable securities and investment firms to hold transactions that are suspected to be related to fraud and financial exploitation for a short period of time while there is an investigation ("report and hold" laws). Almost all states have passed this or a similar law and roughly half of the states have also applied this model to banks and credit unions. Congress could consider a federal law to enable financial institutions to hold suspicious transactions while they investigate them further.

To help curtail gift card scams, AARP's state offices have helped pass comprehensive legislation requiring stores where gift cards are sold to post a notice alerting customers to protect themselves from gift card scams and what to do if they are the victims of this scam, staff training, secure packaging, and record keeping.

AARP has also endorsed a number of pieces of federal legislation in the fraud prevention space, including:

Improving Social Security's Service to Victims of Identity Theft Act (S. 1666)

This bill would streamline and improve the assistance provided by the Social Security Administration to individuals whose Social Security number has been stolen or misused. We thank Chairman Grassley for his leadership on this issue.

The Tax Relief for Victims of Crimes, Scams, and Disasters Act (S.1773/H.R.3469)

Many victims of fraud learn they owe taxes on money that has been stolen from them. This often happens when funds are stolen from their 401(k) accounts. Cashing out a 401(k) account will trigger federal income tax on those funds, as well as an early withdrawal penalty tax if you are under 59 ½. AARP is advocating for the reinstatement of the theft loss deduction and thanks Senator Moody for leading this legislation in the Senate to provide much-needed tax relief to victims.

The GUARD Act (H.R. 2978)

Unfortunately, AARP often hears from fraud victims who find that when they report this fraud to their state and local law enforcement officials, these officers are not able to help as they are not well-equipped to investigate financial crimes. AARP has endorsed the GUARD Act, which would direct federal funding to state and local law enforcement agencies to hire personnel, train staff, and secure tools to fight these crimes, empowering them to combat fraud committed against Americans.

Preventing Deep Fake Scams Act (H.R. 1734)

This bill would establish a dedicated financial services task force on AI to explore the use of AI in the financial sector to commit and detect fraud.

Artificial Intelligence Public Awareness and Education Campaign Act (S. 1699)

This bill would launch a comprehensive public awareness, education, and consumer literacy campaign to educate consumers about the prevalence of AI in their daily lives.

Quashing Unwanted and Interruptive Electronic Telecommunications, or QUIET Act (H.R. 1027)

This bill would improve transparency from robocallers, requiring them to disclose upfront when artificial intelligence is used to imitate human voices in calls or text messages.

Taskforce for Recognizing and Averting Payment Scams (TRAPS) Act (S. 2019)

This legislation would create a task force to combat digital payment scams. The task force—composed of financial regulators, institutions, and consumer advocates—would analyze fraud trends and develop strategies to enhance protections.

Senior Security Act of 2025 (H.R. 1469)

This legislation would help combat financial exploitation of older Americans by creating an interdivisional taskforce at the U.S. Securities and Exchange Commission to examine and identify challenges that seniors face while investing. It would also require the U.S. Government Accountability Office to study and report on the economic costs of the financial exploitation of seniors.

Conclusion

In a world where criminals adapt as fast as technology does, empowering financial institutions with knowledge and authority to stop crimes is not a “nice to have.” It is a “must have.” Based on my experience, it’s clear that the industry is empowered step up to this challenge, they can help stop fraud before it happens, increase public confidence and provide peace of mind for the older adults they serve.

But they can’t do it alone.

Together, policymakers, law enforcement, industry, and most importantly telecom and social media companies can turn the tide against the vicious criminal networks who hold the power right now. Together, we can disrupt their business model, protect millions of consumers and safeguard billions of dollars in savings and retirement accounts and in our economy.

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

Thank you, Senator Grassley and Senator Durbin, for the opportunity to speak with you today.

My name is April Helm. I'm here because my mother, Sherri Tyson, lost \$350,000 to a romance scam before her passing in 2020 while undergoing treatment for late-stage ovarian cancer. It has been a long, frustrating, and heartbreaking journey that has brought me to this moment. And before I share the details, I want to express how surreal it is that I'm sitting here today.

My dad began his career at Kansas Gas and Electric, while my mother started at Farm Bank. She loved her work. Every evening, she came home to cook us a hot meal. We'd sit around the dinner table of our modest brick ranch home, surrounded by a big backyard with a vegetable garden and fresh mint.

As my father moved up the corporate ladder, we moved around Kansas. My mother continued working, eventually becoming the Vice President of a third-party administrator for an insurance company. She was also an entrepreneur. After 25 years of marriage, when I was 19, my parents separated.

Soon after, my mom met my stepfather, John. He was a good man to me and my brother. Life was steady until he passed away from cancer in 2014. My mom remained active, thanks to support from family and friends, but she eventually longed for companionship again. In 2017, during one of my visits, she told me she was going to try online dating.

Within weeks, she sent me a photo of a man named "Gerald." I warned her to be careful and made her promise not to send anyone money. She promised. And yet, over the next few months, I watched my mother fall deeply in love. She was glowing—excited by every message, every interaction. But what we didn't realize was that she was being targeted by a sophisticated criminal network exploiting her vulnerability and her hope for connection.

In 2018, while undergoing cancer treatment, she became even more isolated—and more susceptible. One day, while I was heading to a football game, I received a text from her:

“I gave all my money away. I have nothing. Come get me.”

I was in shock. She had promised. But she had lost her apartment, her car—everything. I told her she could move in with me, but on one condition: she had to stop talking to the scammer. At the time, I didn’t know if these people were in the country or dangerous. She refused. She couldn’t let go of the fantasy they had sold her.

Instead, she moved in with her sister in Mobile, Alabama. When that didn’t work out, she asked me to come get her so she could start fresh in Dallas with my brother. We made a plan to move her that day. But the scammers had another plan—one of their tactics is to keep victims awake all night, exhausted and disoriented.

That morning, as they were preparing to leave, her sister—who is sitting behind me today—found her collapsed on the floor. She never made it to Dallas. I believe, with all my heart, that if it weren’t for the scam, I would have seen my mother that day.

In the early days, there was almost no information online about these scams. As someone with a background in radio news, I launched a podcast to investigate: to talk with other victims, law enforcement, and experts. I’ve interviewed people of all ages and professions who were deceived—smart people: a former CIA agent who lost \$1 million, the son of a marriage counselor, a woman married to a retired colonel, bankers, hospital administrators, investigators.

This crime isn't just happening to the elderly. It's happening to people my age and younger. A woman my age recently made national news after her scam turned her into a money mule, like many do, and she is now facing up to 62 years in prison. I even spoke to the scammers themselves. One told me directly:

"We target Americans because you have money—and slavery."

Many victims go to local authorities only to be told there's no crime because they "gave" the money away. Prosecutors often decline to press charges for the same reason. Victims feel abandoned—penniless, ashamed, and taxed heavily for withdrawing their retirement savings. Some even take their own lives under the weight of the despair.

Today, I serve on the board of **Advocating Against Romance Scammers (AARS)**, a national nonprofit focused on prevention, education, and advocacy. We are pushing for legislation, for tech platform accountability, and for comprehensive victim support. But we can only do so much without federal leadership.

My mother deserved better. Every victim does.

We urgently need Congress to act—to ensure that no more families are shattered by this cruel and complex crime.

Thank you for your time, and for hearing my mother's story.

Joshua M. Bercu Executive Director, Industry Traceback Group

Senior Vice President, Policy, USTelecom — The Broadband Association

Questions for the Record Responses

Scammers Exposed: Protecting Older Americans from Transnational Crime Networks

July 7, 2025

Senator Adam Schiff

- 1. California has the largest population of older adults in the country. Can you share any data or insights on how many California seniors have been affected by transnational scam calls, and how those scams have evolved over time?**

The Industry Traceback Group (ITG) does not have specific data on how many California seniors have been affected by transnational scam calls. In the ITG's experience, however, many scammers have moved from blasting billions of robocalls to more sophisticated, targeted scams. Based on the information we see through traceback as well as public reporting, we know that many of the actors behind these scams are based overseas.

- 2. You mentioned at the hearing that scammers are using AI to generate real-time, responsive fake voices. How has the emergence of AI-generated voice scams impacted ITG's ability to trace back these types of scams? What patterns or sources are emerging?**

To date, the ITG has not seen prolific use of AI-generated voices in data on scam call campaigns we receive from our partners. That said, in the few instances we received examples, the ITG successfully traced such calls without any issue and we stand ready to work with our law enforcement partners to continue to trace back any such calls going forward.

- 3. What policy measures can Congress enact to prevent or detect AI-generated scam calls that mimic trusted voices, such as relatives, government officials, or banks?**

One challenge we face is that the criminals behind AI-generated scam calls will not follow any new law or regulation the government imposes. That said, Congress already has taken an important step in the passing the TRACED Act to reduce fraudsters' ability to impersonate legitimate entities in telephone calls. Among other things, the TRACED Act mandated that providers implement the STIR/SHAKEN call authentication framework. Although it has not completely eliminated spoofing, STIR/SHAKEN has made it far harder for scammers to successfully impersonate legitimate numbers from relatives, banks, or government officials.

In addition, last year, the FCC issued a helpful ruling that calls made with an AI-generated voice are subject to the Telephone Consumer Protection Act's restrictions for calls made with an "artificial voice."

Ultimately, the best tool we have in the toolbox to fully stop scammers is to hold them accountable through cross-border criminal enforcement. As we know, until they are deterred, they will use every available tool and circumvention to seek to defraud Americans at home.

4. How can California’s Attorney General or local law enforcement agencies more effectively coordinate with federal and international partners in scam traceback and enforcement?

The ITG routinely works the Department of Justice, Federal Communications Commission, Federal Trade Commission, state Attorneys General, and increasingly local public safety officials from across the country. Coordination and collaboration, including with peers abroad, is key in our ongoing fight against criminal fraudsters. To ensure effective and efficient coordination across the United States and with international partners, we believe the U.S. Government should establish a national anti-scam strategy with a central coordinator or task force that prioritizes cross-border criminal enforcement. The central coordinator or task force would help to improve coordination, eliminate silos, and give industry a clear point of contact – accelerating action against rapidly evolving threats.

Senator Sheldon Whitehouse

1. Scammers rely on anonymity provided by VPNs and big online platforms to carry out their fraud. What is the best thing we can do to penetrate this anonymity? How can we better hold the big platforms accountable for enabling these kinds of frauds?

The communications industry established the ITG and the industry traceback process precisely to solve for call scammers and spammers’ anonymity – specifically, by spoofing the calls they deliver in mass to U.S. consumers. Each day, the ITG team launches tracebacks to investigate and identify the entities behind illegal calling in order to disrupt their activities and arm the enforcement community to take further action.

Senate Judiciary Committee Hearing
“Scammers Exposed: Protecting Older Americans from Transnational Crime Networks”
Questions for the Record
for Brady Finta
Submitted June 24, 2025

QUESTIONS FROM SENATOR SHELDON WHITEHOUSE

1. Scammers rely on anonymity provided by VPNs and big online platforms to carry out their fraud. What is the best thing we can do to penetrate this anonymity? How can we better hold the big platforms accountable for enabling these kinds of frauds?

You are correct, the technology these sophisticated transnational organized crime groups use to mask their criminal activity often defeats the traditional law enforcement efforts to collect enough evidence to disrupt them. This is why Elder Justice Task Forces (EJTFs) coupled with a public/private partnership on a nationwide scale are so important. Leveraging the ever-advancing technology used by our nation's largest corporations to assist law enforcement in real-time will improve our collective chances to overcome the obstacles put in place by perpetrators. A network of EJTFs around the country will generate the kind of cumulative intelligence and enforcement necessary to define the true scope of the problem. When these EJTFs and their investigations are supported by the National Elder Fraud Coordination Center (NEFCC) and the contributions of the private sector efforts from companies like Google, Amazon, Microsoft, Meta, telecoms and financial institutions, the impact on the elder fraud threat will be real.

In my experience, the anti-fraud departments of many of America's large companies are not only willing, but highly motivated to stop fraud on their platforms. Unfortunately, there has not been a single place for these companies to link their investigations and present cases with this aggregated intelligence. This will be another goal of NEFCC, to pull together these many disparate efforts in one place and offer the results to law enforcement. Impeding this effort to some degree is the perceived liability among our nation's corporations (particularly financial institutions) that sharing information, even on suspected fraud, carries with it enough liability to prevent this kind of collaboration. Offering a clear legislative safe harbor which allows/encourages/requires the sharing of data related to fraudulent activity, not only with law enforcement but with other corporations, would go a long way in solving this problem.

Questions for the Record
Senate Judiciary Committee

“Scammers Exposed: Protecting Older Americans from Transnational Crime Networks”
Sen. Adam Schiff (CA)

Brady Finta, Founder and CEO, National Elder Fraud Coordination Center

1. At the hearing, you mentioned the San Diego Elder Fraud Coordination Center as a proof of concept of the ability to initiate more impactful investigations through localized elder justice task forces using the combined resources of state/local and federal law enforcement. What lessons should Congress take from San Diego to inform a national model?
 1. The San Diego EJTF model should be replicated in every major city in the United States. Not only will there be more than enough cases to work (hundreds of thousands of elderly victims every year and over \$60B in losses), but unless this is accomplished, the efforts of the SD EJTF and the sparse number of individual investigations will have no impact on the overall crime problem.
 2. Not only do the EJTFs need to be created similar to the one in San Diego (Federal, County and Local Law Enforcement, as well as APS), but a local coordination center pulling together the data from the many law enforcement organizations is necessary to understand the scope of the problem and prioritize cases. The value of this has been clear in the Elder Fraud Coordination Cell located in the San Diego County Law Enforcement Coordination Center.
 3. The combined and coordinated efforts of EJTFs around the country involving all levels of law enforcement would create a maelstrom of intelligence and enforcement opportunities.
2. Given California’s size and diversity, what unique challenges or opportunities exist in coordinating across state and federal law enforcement to target transnational elder fraud?
 1. At the moment, there is little to no coordination at all among the many law enforcement agencies located in California with respect to transnational elder fraud. Thankfully, this capability already exists. Every major jurisdiction in California has a Law Enforcement Coordination Center already familiar with deconflicting and coordinating investigations related to drugs, gangs, money laundering and terrorism. Building EJTFs similar to those created for Internet Crimes Against Children (ICAC) task forces, but linked the way California already does for major narcotics investigations would be entirely feasible.
 2. California is already ahead of the ballgame with so much infrastructure, highly trained law enforcement agencies and the example of the San Diego EJTF. I believe California should be a leader in creating EJTFs in its other major cities combining the resources of its state, local and federal agencies.
3. You emphasized at the hearing that many companies already have strong anti-fraud programs, but these efforts are siloed. What types of federal reforms would encourage more collaboration between tech firms, banks, and telecom providers?
 1. In my experience, the anti-fraud departments of many of America’s large companies are not only willing, but highly motivated to stop fraud on their

platforms. Unfortunately, there has not been a single place for these companies to link their investigations and present cases with this aggregated intelligence. This will be a primary goal of the National Elder Fraud Coordination Center (NEFCC), to pull together these many disparate efforts in one place and offer the results to law enforcement. Funding NEFCC to grow enough to support EJTFs around America be a massive force multiplier to those task forces and their investigations.

4. Can you elaborate on how companies, particularly those in California's growing financial and technology sectors, might contribute data to the proposed National Elder Fraud Coordination Center (NEFCC) without compromising consumer privacy protections under laws like the California Consumer Privacy Act?
 1. With investigative departments already designed to detect and investigate fraud, many California corporations are on the cutting edge of this effort. However, their efforts to share the information they have with other corporations who have different pieces of the elder fraud puzzle are stymied by what they see as limitations and liabilities created by privacy laws. New legislation that clarifies and simplifies safe harbor carve outs to allow the sharing of information related to fraud would help tremendously.
5. California is home to one of the nation's largest populations of older adults, many of whom are immigrants or limited-English speakers. How can local elder justice task forces tailor victim outreach and response efforts to serve these diverse communities more effectively?
 1. In our current environment, all communities are underserved with respect to elder fraud. State and local police agencies are not doing any of these cases and federal agencies are not doing enough. The crime is growing at enormous rates and based on law reporting rates, it is clear that the public, regardless of ethnic community affiliation, believes nothing is being done or can be done. A true partnership of state, local and federal law enforcement (via EJTFs), along with the private sector (through NEFCC) and the non-profit partners such as AARP who will spread the word about this comprehensive effort will undoubtedly bring more awareness and encourage more reporting, including in immigrant communities. NEFCC will work directly with the public information departments of the various law enforcement, private sector and non-profit partners to educate and inform all communities of our combined efforts, the need to report, victim services, and prevention.

Senate Judiciary Committee Hearing
“Scammers Exposed: Protecting Older Americans from Transnational Crime Networks”
Questions for the Record
for Jilene Gunther
Submitted June 24, 2025

QUESTIONS FROM SENATOR SHELDON WHITEHOUSE

- 1. Scammers rely on anonymity provided by VPNs and big online platforms to carry out their fraud. What is the best thing we can do to penetrate this anonymity? How can we better hold the big platforms accountable for enabling these kinds of frauds?*

Fraud is a top priority for AARP members. This is unfortunately not surprising given that the FBI [found](#) that fraud victims over the age of 60 had an average of \$83,000 stolen from them in 2024. AARP does extensive fraud prevention and awareness work through AARP’s [Fraud Watch Network](#), which provides consumer education on fraud prevention and we also run a [helpline](#) for victims of fraud. AARP runs the BankSafe Initiative, which is a two-part strategy to get the financial industry to take more substantive actions to stop financial exploitation and better meet the needs of older adults. One part of BankSafe focuses on training frontline staff—often the only people positioned to recognize and stop exploitation before funds leave the account. The second part creates system-level changes inside financial institutions—aligning day-to-day operations, business-processes and transaction protocols with stronger consumer protection.

As you highlight in your question, criminals adapt quickly to new technologies (like cryptocurrency, payment apps, anonymity-enhancing technology), and it is likely that this has been the case with VPNs. When criminals use VPNs and large online platforms to mask their identities, but this anonymity is not absolute. One way to pierce it is by monitoring IP address ranges used repeatedly in fraud incidents and sharing that data across platforms and institutions. Increased transparency—such as retaining and disclosing information about repeat offenders and suspicious activity—could also help. Federal guidance on consistent accountability standards could also prove helpful. AARP believes these technologies can also be used by the general public to protect themselves from fraud and have encouraged consumers to leverage these same technologies to protect themselves. For example, here is advice we shared in an [article](#) on staying safe while web browsing:

5 tips to remain private

1. Avoid public Wi-Fi hotspots in places such as airport lounges, coffee shops or hotel lobbies. You never know if your information is being tracked and logged, so wait until you get home. If you can’t wait, use your smartphone as [a personal hotspot](#), but be aware it requires a data plan.

2. When you [install an app](#) on an Apple device such as an iPhone, tap to agree [not to let apps track](#) your whereabouts online. This reduces an app’s visibility into your web browsing and app activity. If you allow tracking, sites such as Facebook could know

where you recently searched, like visiting a home improvement store site for power tools. This increases the odds of your seeing Facebook ads tied to power tools in the future.

3. Use [a strong password](#) for all your accounts, at least eight characters and a combination of letters, numbers and symbols plus upper- and lowercase letters. Never use the same password for all online activity. Better yet, install [a password manager](#). And opt for two-factor authentication, also called multifactor authentication, which requires a password and one-time code typically sent to your mobile device.

4. Make sure you have [good antivirus software](#) to stop threats. Turn on automatic updates for your devices, web browsers and third-party add-ons. They warn you of suspicious websites you may find yourself in.

5. Opt for a screen guard, also known as a privacy screen, if you frequently use your laptop outside the house. You'll need to find one that fits your screen perfectly, such as a 15-inch screen with 16:9 aspect ratio, and learn to look straight at the laptop to see words and images. For everyone else, like the guy in the seat next to you on a plane, the screen looks as if the computer is turned off.

We would be happy to discuss potential policies to encourage technology platforms to better prevent their platforms from being used to enable fraud with your office.

Senate Judiciary Committee Hearing
“Scammers Exposed: Protecting Older Americans from Transnational Crime Networks”
Questions for the Record
for April Helm
Submitted June 24, 2025

QUESTIONS FROM SENATOR SHELDON WHITEHOUSE

1. Scammers rely on anonymity provided by VPNs and big online platforms to carry out their fraud. What is the best thing we can do to penetrate this anonymity? How can we better hold the big platforms accountable for enabling these kinds of frauds?

Questions for the Record
Senate Judiciary Committee
“Scammers Exposed: Protecting Older Americans from Transnational Crime Networks”
Sen. Adam Schiff (CA)
April Helm, Host, Scammer Stories Podcast

1. You noted at the hearing that tech platforms have a responsibility to bear for enabling the scams that devastated victims like your mother. What specific actions should Congress consider requiring of online dating or social media companies to detect and prevent romance scams?
2. You described launching your podcast due to the lack of public information. What federal or state-level public education campaign would have made a difference for your family, and what messaging have you seen victims respond to best?

A federal education campaign, that includes survivor stories, works best in getting the message through to victims and showing that they are not alone. However, it is often difficult to stop a scam once the scammer gets their hooks into someone. Awareness campaigns before the crime begins is key and we need to get started right away.

Require platforms to run educational content on the common signs of scams and how to report them.

Clear regulations can hold platforms accountable to report and remove scams swiftly. Right now, there is very little movement in this area with no incentive for platforms to take any action. Fines need to be added for scamming accounts.

Detection tools are now easier than ever with artificial intelligence on tracking scam patterns and behavior. Platforms need to be held accountable for criminal activity on their sites by updating the Telecommunications Act of 1996.

Platforms should all put a system into place with stronger identity verification so people's pictures aren't stolen.

Limit how often new accounts can message others without being friends/followers. Flag messages that use romance scam tropes.

Also, there is some international coordination today, but clearly not enough. We need an increase in exchanged informational between law enforcement and the banking industry.

This is a foreign policy issue that will take a whole-of-government-approach with law possible sanctions.

A P P E N D I X

The following submissions are 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
LoveSaid, 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> , news article	56
---	----

