Testimony of

Kathy Stokes
Senior Director, Fraud Prevention Programs
AARP Fraud Watch Network

on
The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters
before the

U.S. Congress Joint Economic Committee
March 25, 2026

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

My name is Kathy Stokes, and I am Senior Director of Fraud Prevention Programs for the AARP Fraud Watch Network. I am honored to be here to testify on behalf of AARP, which advocates on behalf of 125 million Americans age 50 and older and their families. I would like to thank you and the members of the U.S. Congress Joint Economic Committee for holding this important hearing, "The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters." AARP has long worked to educate consumers, support fraud victims, and improve fraud detection and prevention across industries, and we look forward to working with you towards policy solutions to prevent fraud and protect consumers.

***AARP Fraud Prevention Work***

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

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

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

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

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

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

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

***The Fraud Crisis***

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

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

***The Criminals Behind Fraud***

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

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

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

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

***Why Scams Succeed***

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

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

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

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

***Concerning Fraud Trends***

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

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

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

**Tech Support Scams**

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

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

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

**Bank Impostor Scams**

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

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

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

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

**Financial Grooming**

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

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

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

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

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

**Cryptocurrency Kiosk Scams**

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

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

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

Older adults are disproportionately affected by fraud and scams using cryptocurrency kiosks. In the first eleven months of 2025, the FBI received reports of $333 million stolen in cryptocurrency kiosk scams. This is a significant increase from 2023, when the FBI received over 5,500 complaints involving crypto kiosks, and Americans reported over $189 million in stolen funds – and we know from FTC analysis that these figures represent just the tip of the iceberg. Additionally, over 65% of the theft losses in cryptocurrency kiosk fraud were experienced by adults 60+. AARP is advocating for important consumer protections that will deter criminals from leveraging cryptocurrency kiosks in their schemes. We are leading state-level advocacy that has driven the enactment of consumer protection laws in 18 states, establishing requirements for fee and exchange rate transparency, fraud warnings, and transaction limits. That effort continues this year advocating to pass legislation already introduced in 20 additional states.

And our work doesn't stop there. We are also advocating at state capitals for protection against other ways criminals steal money, like gift card fraud and deed fraud, additional money for law enforcement, and ways to return stolen money back to victims through restitution funds. This will help prevent older Americans from losing their life savings they worked so hard to amass.

***A Path Forward***

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

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

For educators, it is important that we tell consumers about the signs of the latest scams and their red flags. But what if we are able to come up with something simpler? If we can train our brains on how most scams come at us and what to do when they do, we could probably thwart a great deal of crime before it happens. Most scams come as a communication out of the blue that gets

us immediately into a heightened emotional state and contains urgency. If we could train consumers that this scenario is likely a scam, we can train them how to react. AARP launched a campaign last summer that we call “Pause, Reflect, Protect” and we encourage others with fraud education campaigns to adopt the concept and the language.

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

From a public policy perspective, there are many actions Congress can take to address the fraud crisis and we are grateful to the many members of the Joint Economic Committee who are working on legislation to address these issues.

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

Senator Moody is leading and Representative Min has cosponsored S. 1773/H.R. 3469, the Tax Relief for Victims of Crimes, Scams, and Disasters Act. This legislation would reinstate the casualty and theft loss deduction, better ensuring fraud victims don't have to pay taxes on stolen funds. Currently, if you have money stolen from retirement or other taxable accounts the IRS may tax you on money you already lost to criminals. The current policy essentially revictimizes Americans who already had their hard-earned savings stolen from them. This legislation will help end the injustice currently written into the tax code.

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

AARP is also grateful to Ranking Member Hassan for cosponsoring S.2950, the Scam Compound Accountability and Mobilization Act (SCAM Act). Many scams are perpetrated by transnational criminal organizations operating compounds overseas, with trafficked individuals coerced into defrauding Americans under duress. The SCAM Act will bring together federal

agencies, law enforcement, and international partners to develop and implement a comprehensive strategy to counter scam compounds.

Ranking Member Hassan and Senators Moody and Kelly have cosponsored S. 2501, the Veterans Scam and Fraud Evasion (VSAFE) Act. The bipartisan VSAFE Act strengthens the federal government's ability to protect veterans and military retirees from increasingly sophisticated fraud schemes by establishing a Veterans Scam and Fraud Evasion Officer within the Department of Veterans Affairs. This dedicated official would serve as a centralized leader responsible for preventing, identifying, and responding to scams targeting veterans, improving coordination across VA offices and enhancing collaboration with other federal agencies. By improving communication, incident response, and accountability, the VSAFE Act will help safeguard veterans' financial security, benefits, and well-being while addressing the growing threat of fraud aimed at those who have served our country.

Ranking Member Hassan, Senator Klobuchar, and Representative Beyer have all cosponsored S. 2019/H.R. 4936, the Taskforce for Recognizing and Averting Payment Scams Act (TRAPS Act), which aims to protect older Americans from financial scams. The task force—composed of financial regulators, institutions, and consumer advocates—would analyze fraud trends and develop strategies to enhance protections.

Senator Klobuchar has cosponsored S. 3774, the Safeguarding Consumers from Advertising Misconduct Act (SCAM Act). The SCAM Act requires online platforms to verify advertisers, prevent the use of stolen or synthetic identities, and deploy robust fraud-detection tools, including impersonation-detection programs and both automated and manual review processes. It implements user-friendly reporting mechanisms so consumers can quickly flag suspected scam ads and ensures timely platform action. The bill also directs the Federal Trade Commission to issue regulations within one year, update them annually, and enforce violations as unfair or deceptive practices under the FTC Act. Additionally, it empowers State Attorneys General to take action and provides a private right of action for consumers harmed by fraudulent advertisements.

Committee members Senator Budd and Representative Min have sponsored S.2666 and H.R. 6152, the Foreign Robocall Elimination Act. This bipartisan legislation builds on the TRACED Act and represents a critical next step in protecting Americans—especially older adults—from fraudulent and abusive robocalls originating outside the United States. Older Americans are disproportionately targeted by these scams, which often result in financial loss, identity theft, and emotional distress. The bill would establish an interagency task force led by the FCC, FTC, and DOJ to study call volumes, identify high-risk countries, evaluate consumer harm, and promote global adoption of call authentication technologies like STIR/SHAKEN.

Senator Kelly introduced S. 1699, the Artificial Intelligence Public Awareness and Education Campaign Act, which would launch a comprehensive public awareness, education, and consumer literacy campaign to educate consumers about the prevalence of AI in their daily lives. This bill supports AARP's goals of enhancing the safe adoption of new technologies by older Americans. Empowering older Americans with this information will not only help protect against fraud and abuse but also unlock the positive potential for AI to improve daily tasks.

Committee members Representative Smucker and Senators Klobuchar, Heinrich, and Kelly all sponsored S. 1467, the Homebuyers Privacy Protection Act. This bipartisan legislation – now law – takes important steps to protect older Americans—who make up more than 75% of U.S. homeowners—from misleading and fraudulent solicitations during home transactions. By requiring consumers to opt in before their credit inquiry data can be sold and limiting the use of mortgage "trigger leads," the bill helps prevent scams that exploit major life events like buying or selling a home.

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

AARP has urged Congress to strengthen fraud reporting systems so law enforcement can better prioritize and connect cases. While the FBI's Internet Crime Complaint Center (IC3) is the central reporting hub for cyber-enabled crimes, limited analytics and system interoperability prevent the FBI from identifying patterns or links across reports and other databases. As a result, related crimes may appear too small to trigger investigation. AARP is advocating for upgrades that make IC3 data searchable and linkable to enable law enforcement to build larger, more impactful cases.

We also believe that it is important to streamline victim reporting, which is currently received by agencies on an agency-by-agency basis, leaving victims confused about who to report to. This is critical because fragmented and confusing reporting systems prevent authorities from seeing the full scope and patterns of fraud. When reports are scattered across agencies or lack standardized data, related crimes can appear isolated and fall below investigative thresholds, allowing organized criminal networks to operate undetected. A clear, accessible reporting process improves data quality, enables faster triage and coordination, and ultimately increases the likelihood that cases are investigated, perpetrators are held accountable, and future victims are prevented.

Improving victim restitution must be a core component of our response to fraud, because for many victims – especially older adults – the financial losses are devastating and often irreversible. Too often, victims face complex, slow, or opaque processes to recover even a portion of what was stolen, and in many cases receive nothing at all, compounding the harm they have already suffered. Congress can help by strengthening mechanisms that prioritize returning seized and forfeited funds to victims, removing tax penalties that effectively punish those who have been defrauded, and ensuring agencies have clear authority and resources to assist victims in recovery. Meaningful restitution not only helps victims regain financial stability and dignity, it also reinforces trust in our systems and sends a clear message that the government stands with victims.

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

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

Fraud is a complex and evolving threat, but it is not insurmountable. By empowering individuals with practical protections, equipping educators and industry with clear prevention strategies, and advancing smart, coordinated public policy, we can significantly reduce the harm these crimes inflict on Americans. Protecting Americans from fraud is not only possible, it is essential to financial security and economic trust.

***Conclusion***

Scams are not a series of isolated crimes – they are a global, industrialized threat that drains household wealth, fuels transnational criminal organizations, and undermines confidence in our financial and economic systems. The status quo is failing victims and empowering criminals who exploit fragmentation, jurisdictional gaps, and outdated tools. If left unchecked, this crime will continue to erode retirement security, strain public safety nets, and siphon billions of dollars from the U.S. economy each year.

But this crisis is not inevitable. Congress has a clear opportunity – and responsibility – to modernize our national response by strengthening coordination across agencies, equipping law enforcement with the tools and data they need, holding industry accountable for prevention, and ensuring victims are treated with dignity, compassion, and meaningful restitution. When fraud is recognized as the serious economic and national security threat that it is, and when we act together with urgency and resolve, we can disrupt criminal networks, protect Americans' life savings, and restore trust in our systems.

AARP stands ready to work with this Committee and the full Congress to help turn the tide – because protecting Americans from fraud is not only achievable, it is essential to financial security, economic resilience, and the integrity of our nation.