Testimony of

Jilenne 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 Jilenne Gunther, and I am the National Director of AARP's Bank*Safe* 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 Bank*Safe* Initiative is a business-to-business (B2B) solution centered on working with the financial industry to stop financial exploitation before money leaves the account. Bank*Safe* 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.

Bank*Safe* 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 units, investment firms, retailers selling gift cards, and the P2P providers) to implement industry-wide safeguards and policies that better protect consumers. Bank*Safe* provides a suite of offerings to help the industry prevent financial exploitation. These most often include:

- **Training.** Among Bank*Safe'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, Bank*Safe* 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, Bank*Safe* 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.** Bank*Safe* 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 Bank*Safe*-modeled policy changes to better protect consumers.

- **Promising Practices.** As part of our work, Bank*Safe* 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 Bank*Safe* 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 Bank*Safe* training saved 16 times more money than those without the training. Based on these findings, we estimate that Bank*Safe* 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 Bank*Safe* 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 Bank*Safe* 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 Bank*Safe* video that she had watched. She said, "I was so nervous when I started to see the red flags. [The Bank*Safe* 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 Bank*Safe* 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.

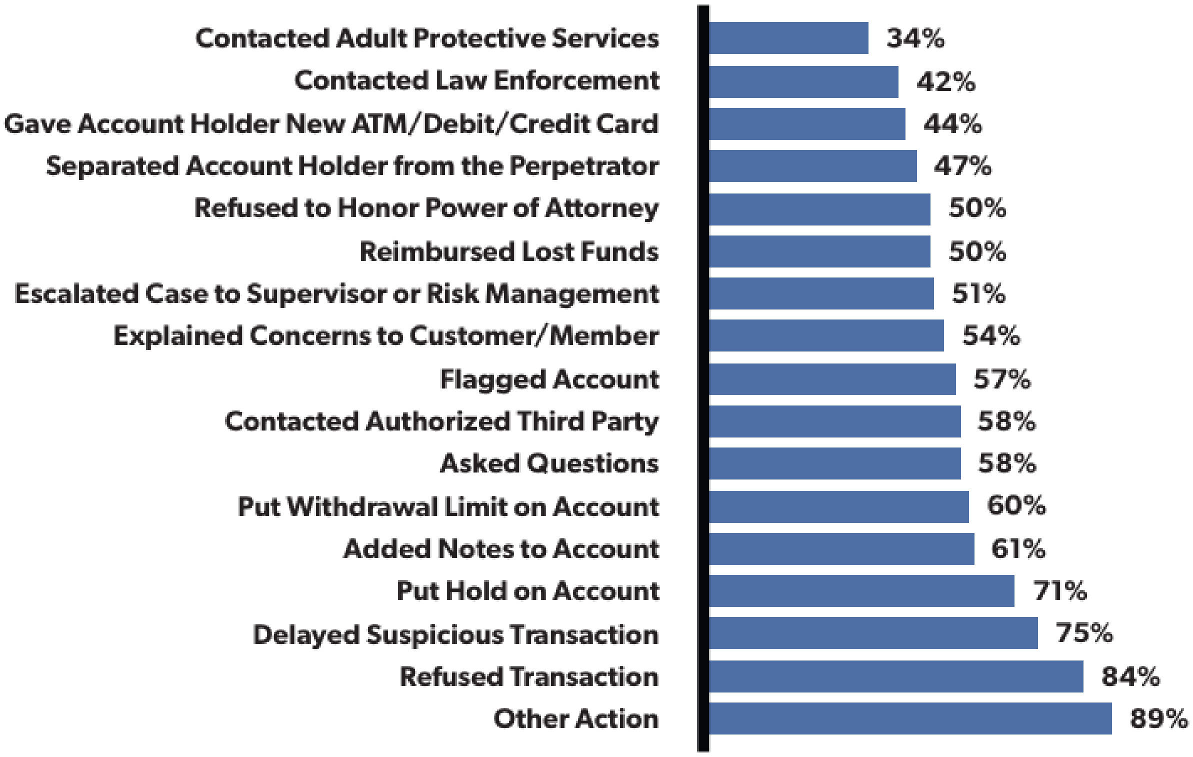
Proven Industry Interventions

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 Bank*Safe* 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 are 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 polices, 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.