



Testimony of

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

On

Safeguarding Main Street: Combatting Fraud and Exploitation in our Capital Markets

Before the

United States House Committee on Financial Services
Subcommittee on Capital Markets
April 15, 2026

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 House Committee on Financial Services Subcommittee on Capital Markets for holding this important hearing, "Safeguarding Main Street: Combatting Fraud and Exploitation in our Capital Markets." 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 in Missouri 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. My work over the past few decades has been replicated in over 40 states and cited in reports by federal agencies like the CFPB and GAO. 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 older and vulnerable adults. We've worked with 1,500 financial organizations across six financial industry subsectors, and our program has helped save more than an estimated \$560 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 worked in the financial industry. 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, who also worked in the financial industry, recognized the red flags. And in a move only someone in the industry 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 or wealth advisors in their family. They don't have access to dye packs. That experience lit a fire within me. I built a fraud prevention program at the very institution 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 is that 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 2025, with an average loss of \$38,500 for those age 60-plus reporting a fraud loss, compared to \$20,699 for all ages. Fraud doesn't need to originate in the securities industry to impact investment accounts. In many cases, it ultimately leads to the sale of assets and transfer of funds out of those accounts. Financial institutions can see the magnitude of this activity through required reporting. In its 2024 review of Bank Secrecy Act filings tied to elder financial exploitation, the Financial Crimes Enforcement Network [identified](#) 155,415 filings over a one-year period, representing about \$27 billion in reported suspicious activity across both attempted and completed transactions. The agency also emphasized that these losses extend beyond checking accounts, frequently affecting retirement savings and investment portfolios as well.

Scams are now a routine part of daily life for many Americans and an escalating concern for both consumer protection and national security. A majority of U.S. adults [report](#) encountering scam attempts on a regular basis, whether by phone (68%), email (63%), or text (61%), with about one in three also seeing them on social media.

The impact is significant. Nearly half of adults [say](#) they have already taken some form of action in response to a scam, such as sharing personal information, sending money, or engaging with a fraudulent investment opportunity.

The scale of the problem is also growing. The Federal Trade Commission [data](#) shows that reported fraud losses to the Sentinel database have increased 27% from 2024 to 2025, and broader research indicates the global scam economy is now comparable in size to the illicit drug trade.

Criminals often target older adults because they have more money — they have spent a lifetime accumulating 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 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, investment firm, 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 victim knows. In these instances, perpetrators take advantage of their long-established relationship with the victim 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 of exploitation.

Reported cases vary, as evidenced by 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.

The problem with relying on self-reported data is that there are massive rates of underreporting among instances of financial exploitation, which vary widely. 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.

AARP is currently conducting a study to measure the underreporting rate of financial exploitation, which we hypothesize will show an even larger annual loss among older adults. The current data shows that many people do not self-identify that they have even been a victim of a crime.

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 investment firms, banks, credit unions, 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. During these qualitative interviews we found that 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 also 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 1,500 financial institutions across six subsectors (investment firms, banks, credit units, 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 like financial advisors (those managing potentially suspicious transactions as well as those having personal interactions with consumers), who are often in the best position to identify red flags and stop exploitation, is crucial. Unlike many existing training courses 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 to intervene in suspicious transactions (or what the industry refers to as risk-mitigation steps), and information on how to spot cognitive decline in consumers.

- **Internal policies and procedures.** BankSafe provides financial institutions and staff with policy templates and guidance to help them delay, hold or refuse suspicious transactions. Included in these materials are recommendations for suspicious-incident documentation, escalation procedures, AI-based alerts, 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. These are real strategies financial institutions are using to prevent exploitation. We engage directly with industry leaders, investment firm executives, financial advisors 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 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 \$560 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. Another mid-sized wealth management firm with roughly 1,500 financial advisors applied AARP training to detect and intervene in suspicious activity, helping prevent an estimated \$14 million in losses in a single year.

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 clients associate with their investment and financial

relationships. Wealth advisors, call center agents, fraud risk managers, 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. Investment firms 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 are better at preventing exploitation and protecting older adults before money ever leaves the account.

Ability to hold suspicious transactions

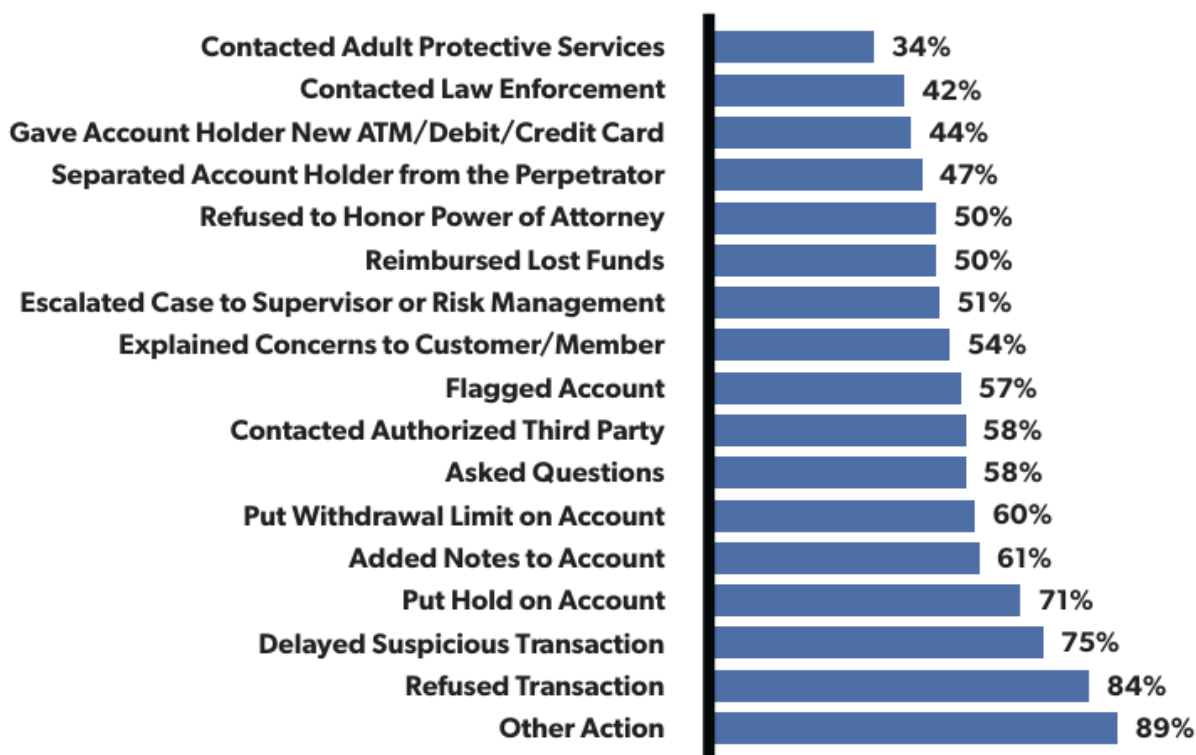
AARP supports policies that allow securities and investment firms to temporarily hold transactions suspected of financial exploitation while an investigation is underway (“report and hold” laws). FINRA Rule 2165 gives firms a tool that matters in elder fraud: it creates time to investigate and escalate before a pressured liquidation turns into an irreversible transfer. Rule 2165 creates a national standard that permits a firm to place a temporary hold on a disbursement or a securities transaction for a ‘Specified Adult’ when it reasonably believes exploitation occurred, is occurring, has been attempted, or will be attempted. The hold framework includes time limits and extensions up to a total of 55 business days when the firm reports to a state regulator or agency or court and the reasonable belief persists. Compared to other sectors, investment firms have been ahead of the curve in adopting these protections, demonstrating how proactive industry leadership and the public sector can create a clear win-win — empowering institutions to act while strengthening safeguards for consumers. In fact, in a groundbreaking random control [study](#) conducted by Virginia Tech of nearly 200 financial institutions, denying and holding a transaction was one of the top three risk mitigation strategies to stop exploitation before the money left the account.

Empowering the front lines

Preventing financial exploitation begins where it most often occurs: at the point of transaction. Investment firms and other financial institutions that prioritize frontline intervention are seeing real impact. Training wealth advisors, call center representatives and other consumer-facing 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. This is especially critical in investment settings, where a single transaction, such as liquidating a brokerage or retirement account, can represent a lifetime of savings.

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 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. This innovation was the product of conversations I had with my father, who was also in the industry, which is just one example of public-private collaboration leading to solutions that better protect consumers.

Similarly, Trusted Contacts is a solution created with industry collaboration that allows 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 tell 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 artificial intelligence (AI), machine learning and technology for proactive protection

The threat of AI is evolving quickly. The growth of real-time payment systems is enabling scams to move faster, reach more people, and appear increasingly convincing. According to [the FBI](#), cryptocurrency investment fraud alone accounted for more than \$11.3 billion in reported losses in 2025.

These incidents are not occurring in isolation. Transnational criminal networks, including organized crime groups, and in some cases, state-linked actors, are systematically targeting U.S. consumers. As a result, fraud is no longer just a consumer protection issue. It is an economic and national security challenge with broad implications.

At the same time, advancements in AI and predictive analytics are creating new opportunities for earlier, more effective intervention. Financial institutions can use these tools to detect out-of-pattern activity that may signal scams, often before losses occur. For example, AI-powered systems can analyze transaction behavior, communication patterns, and account activity to flag inconsistencies in real time. Emerging tools also allow consumers to check suspicious texts, emails, or calls against databases of known scam tactics, capabilities that could become a standard layer of defense.

Monitoring analytics can also show indicators of identity theft, such as accounts opened under suspicious conditions or inconsistent identity signals. More advanced predictive models can establish a baseline of typical customer behavior and flag meaningful deviations, such as irregular deposit activity, unusual transaction timing, or even changes in how a user interacts with digital platforms.

In some cases, these signals extend beyond fraud detection. Research suggests that sudden shifts in financial behavior, combined with other indicators like credit profile changes, can correlate with cognitive decline, including conditions such as dementia, years before clinical diagnosis. While still emerging, these insights point to a future where financial data can support not only fraud prevention, but broader consumer protection and well-being.

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. With the largest wealth transfer set to take place, this puts consumers and the industry in critical positions. The industry can mitigate losses 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 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 reduce the industry's ability to fully protect the nation's most vulnerable consumers.

Sharing information across the industry, telecom and social media companies

Even when fraud is suspected, financial institutions are 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 from 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. We can close that gap without broad data expansion by sharing narrow, time-sensitive exploitation indicators under clear guardrails.

Breakdowns in information sharing can have significant consequences in the securities industry. One firm may notice a client rapidly selling off long-term holdings, while another bank processes transfers to a newly created account, and a telecom provider detects a spike in suspicious calls. Viewed in isolation, each signal may not trigger action. But together, they point to a clear pattern of potential fraud.

If institutions were able to exchange focused, relevant data in real time, such as indicators of unusual activity, emerging scam tactics, or accounts already flagged as high-risk, they could identify these patterns much earlier. Even a small window of added time can be critical, allowing firms to escalate internally, notify a trusted contact, or pause a transaction before funds are lost.

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 must look upstream to 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 during a wire transfer or divestment, but earlier, before the consumer enters the psychological state of panic, fear, or urgency that criminals count on. Once someone is in "fight-or-flight" mode, rational decision-

making narrows, making interventions much harder. Acting early means spotting risk before funds are moved out of an investment account. Indicators might include unexpected asset sales, new transfer requests or subtle changes in a client's behavior that suggest outside influence. When firms proactively monitor for these signals and give advisors the ability to step in — whether by pausing activity or probing further — they can often stop fraud before any money leaves the account. After a transfer occurs, particularly across institutions or into crypto or international channels, recovery becomes far more difficult.

That's what makes this stage so important. It's one of the few points where timely action can meaningfully prevent losses altogether.

With the explosive growth of telecommunications and social media over the past two decades, it's no longer enough to focus prevention solely on the financial industry. 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 advertisement authenticity checks, along with enforcement procedures for removing fraudulent advertisements, could 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 and even telecommunications, not just financial institutions. 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 United Kingdom (UK) to speak to industry leaders about this very opportunity. The industry in the UK is in some ways more advanced when it comes to regulations and industry-led initiatives to protect vulnerable groups. Successful [pilot programs](#) in the UK show that sharing across sectors can surface scam threats a day or more earlier than bank-only systems. 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.

Platform accountability and credentialing

Countries like Australia, Singapore 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 to do so. Now, in the UK, platforms are required to verify that financial advertisers are authorized before allowing promotions, reducing exposure to fraudulent investment schemes. This highlights the problem: without investment firms,

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. At worst, we are enabling criminals because we do not work together as one system. There is not one lead federal agency tasked with coordinating our response. A key vulnerability today is how easily bad actors can access platforms and reach consumers with little verification. Stronger, more consistent credentialing is essential to reducing fraud at scale.

Companies and government agencies should expand identity and business verification standards by applying "know your customer" principles to digital platforms, advertisers, and marketplaces. Platforms should more rigorously vet participants at onboarding and over time, including verifying business identity and, where appropriate, requiring proof of licensing. Higher-risk categories should carry enhanced standards to prevent fraudulent actors from reaching consumers in the first place.

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 financial institutions, 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.

AARP Advocacy

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 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.

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. Stores are also required to conduct staff training, secure packaging, and record keeping.

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

The GUARD Act (H.R. 2978/S. 2544)

Unfortunately, AARP often hears from fraud victims who find that when they report this fraud to their state and local law enforcement officials, the officers are not able to help as they are not well-equipped to investigate financial crimes. AARP has endorsed the

GUARD Act, led by Senator Britt in the Senate. This bill 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.

STOP Scams Against Seniors Act (H.R. 6426)

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.

Financial Exploitation Prevention Act (H.R.2478/S.2840)

This legislation would allow registered open-end investment companies (mutual funds) and transfer agents (typically a bank or trust company that acts as an intermediary between a company (or fund) and its investors) to delay the redemption of securities when there is a reasonable belief that the request was made due to financial exploitation of an investor. AARP has advocated for similar laws across the United States, and thanks to our advocacy work, 43 states now have report-and-hold laws applying to the securities industry, and 26 have them applying to banks. This legislation builds on that work by providing critical tools to protect the lifesavings of older Americans from potential fraud and exploitation.

Preventing Deep Fake Scams Act (H.R. 1734/S. 2117)

This legislation will establish a dedicated task force on AI in financial services that would include representatives from key financial services regulatory agencies, financial institutions, third-party vendors, and AI experts to explore the use of AI in the financial sector to combat 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.

Taskforce for Recognizing and Averting Payment Scams (TRAPS) Act (H.R. 4936/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/S. 4055)

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 investment firms and other 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 to 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.