Testimony of

Kathy Stokes
Director of Fraud Prevention Programs
AARP Fraud Watch Network

on

Following the Money: Tools and Techniques to Combat Fraud

before the

U.S. House Financial Services Committee
Subcommittee on National Security, Illicit Finance, and International Financial Institutions

April 1, 2025

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

My name is Kathy Stokes, and I am the 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 for the more than 100 million Americans age 50 and older. I would like to thank you and the members of the House Financial Services Committee for holding this important hearing, "Following the Money: Tools and Techniques to Combat Fraud." 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 fraud victims.

AARP Fraud Prevention Work

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.

We show up 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.

Beyond education, 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, from 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.

AARP has also 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. This must change if we are to meaningfully combat this insidious and devastating crime.

Additionally, AARP is proud to be among the founders of the new nonprofit National Elder Fraud Coordination Center (or NEFCC) which formally launches this month. Similar to the National Center for Missing and Exploited Children, this private/public partnership will aggregate and analyze private and public sector fraud data through an organized crime lens, tying cases together to produce data-rich packages for federal law enforcement investigation and prosecution.

The Fraud Crisis

The growth in fraud crimes over the past five years has been meteoric. For example, published report data from the Federal Trade Commission (FTC) shows a reported $12.5 billion stolen in 2024. But this number doesn't begin to tell the true story. In a 2024 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 2023 was not the reported $10.4 billion, but more like $158.3 billion. And the agency pegged fraud losses among older adults at $61.5 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 most of the fraud we see today. Importantly, the funds they amass by stealing billions of dollars through fraud represents 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* recently 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 becoming a fraud victim is not the victim's fault. They didn't become a victim because of their age, educational level or cognitive impairment. They became a victim because of how our brains function.

This message is critical if we are ever 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 and 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 their bank's fraud investigator, and their accounts are actively being 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 ATM 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 look like bank ATMs and allow people to conduct legitimate cryptocurrency transactions, such as sending money to digital wallets. Today, there are more than 45,000 crypto ATMs nationwide. However, because crypto ATMs 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 crypto ATMs 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 ATM. It is then transferred to a digital wallet controlled by the criminal.

Older adults are disproportionately affected by fraud and scams using cryptocurrency ATMs. In 2023, the FBI received over 5,500 complaints involving crypto kiosks, and Americans reported over $189 million in stolen funds. 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. Our state-level advocacy recently led to the passage of a bill in Nebraska to put important consumer protections, including fee and exchange rate transparency, fraud warnings, and transaction limits in place.

This will help prevent older Americans from losing their retirement 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 has been working on this concept with input from people around the globe and are hopeful something can be accomplished.

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.

For example, we are very pleased that Representative Zach Nunn (R-IA) has reintroduced legislation, 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.

AARP has also urged Congress to improve fraud reporting systems to ensure that law enforcement can adequately prioritize cases. The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) is the central site for reporting cyber-enabled crimes. Currently the FBI generally does not have advanced analytics capacity or interoperability across FBI systems. The result is that the FBI cannot identify commonalities between reported crimes

and cannot search these reports to compare with information in other systems. Without the ability to analyze information to identify the most commonly reported identifiers or between systems, the FBI cannot easily find potential links between cases. Ultimately this could lead to a situation in which the severity or extent of a crime is not recognized and perhaps not properly reviewed because it appears to be under a threshold for investigation. We are advocating for the FBI to prioritize enhancements to its data systems so that IC3 reports can be easily searchable and analyzed for potential links.

AARP is also advocating for the reinstatement of the casualty and theft loss deduction. The impact of fraud often goes beyond the theft of funds – if a criminal has stolen funds from a victim's 401(k) or other taxable account, this is considered a taxable event and the victim will likely owe taxes on the funds withdrawn from the account, and often end up in a higher tax bracket, compounding the loss. This an insurmountable burden for many victims, many of whom no longer have the ability to pay this tax bill due to the fraud loss. It can also impact a victim's eligibility for public benefits based on income. As of 2018, theft losses are no longer covered under the tax code and casualty losses are only covered if the loss is due to a major disaster as declared by a Presidential disaster declaration. There have been several pieces of legislation introduced in Congress to reinstate the casualty and theft loss deduction and AARP urges Congress to restore the deduction in any upcoming tax package.

Industry and law enforcement should champion the success of the new National Elder Fraud Coordination Center (NEFCC), noted earlier. 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.

Policymakers have an important role to help victims and bring the fight to fraud crime rings, including legislative solutions such as: providing more resources to train state and local law enforcement to investigate fraud crimes; reinstating the casualty loss deduction to address the significant tax burden that fraud victims face having to also pay taxes on the assets that were stolen; limiting the damage of fraud involving cryptocurrency ATMs; improving staffing of DOJ's Elder Justice Strike Forces; and enhanced efforts such as the National Elder Fraud Coordination Center to bring the public and private sectors together to build cases for investigation and prosecution.

Conclusion

Addressing fraud requires more than piecemeal solutions; it demands a whole-of-society approach. We cannot educate our way out of the fraud crisis. Industry cannot mitigate and engineer our way out of it. Policymakers cannot regulate our way out of it. And law enforcement cannot arrest our way out of it.

But, together, educators, policymakers, law enforcement and industry can turn the tide against the vicious crime gangs 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.