# Safeguarding retirement in the age of scams

TIAA Institute

# Contents

# Executive summary

Millions of older Americans are targeted by scams and fraud every year, jeopardizing their retirement security. Scams are a type of mass marketing fraud that use low-cost communication methods such as email, text, social media and telephone calls to fraudulently solicit numerous prospective victims through false representations and deceit. Nearly 400,000 fraud and scam complaints by adults age 60 and older were reported to the Federal Trade Commission (FTC) in 2023, reflecting $1.9 billion in total losses.[1] Many of these complaints involved government, bank and business imposters, investment schemes, fake sweepstakes and lotteries, tech support scams, and romance scams, with new variants emerging every day.

Older adults are intentionally targeted by scammers[2] and experience a higher risk of repeat victimization.[3, 4] A meta-analysis combined data from multiple studies and found that 5.4% of older Americans are victims of one or more fraud schemes every year.[5] Several factors associated with aging are believed to increase older adults' risk of victimization, such as greater wealth accumulation, lower technological sophistication, social isolation and loneliness, and declines in cognitive functioning. However, because scam messages are tailored to different age groups and subpopulations, people of all ages and backgrounds are at risk.

Although fraud is vastly underreported,[6, 7] older victims who file complaints typically report much higher median losses compared to younger victims—$1,450 for those age 80 or older compared with less than $500 for those ages 20 to 59.[8] This suggests scams inflict more financial harm on a population that has largely exited the labor force, severely limiting their ability to financially recover. In addition to financial costs, the psychological and emotional consequences of victimization can be severe. Scam victimization is highly stigmatized and often results in shame, embarrassment, isolation and a loss of trust.[9–14]

The financial services industry—along with retirement plan sponsors and plan participants—can take steps to reduce the likelihood of scam victimization but, they are not alone in this battle. Retirement plan providers can harness new technology to authenticate plan participants, secure their accounts, flag suspicious transactions, elevate awareness and advocate for increased protection. Plan sponsors can educate employees to be watchful for red flags that help them detect fraud and encourage their adoption of account security features. Meanwhile, plan participants can educate themselves on the hallmarks of scams and add trusted contacts to their financial accounts. Those trusted contacts can act as financial advocates and help oversee the plan participants' accounts as they age.

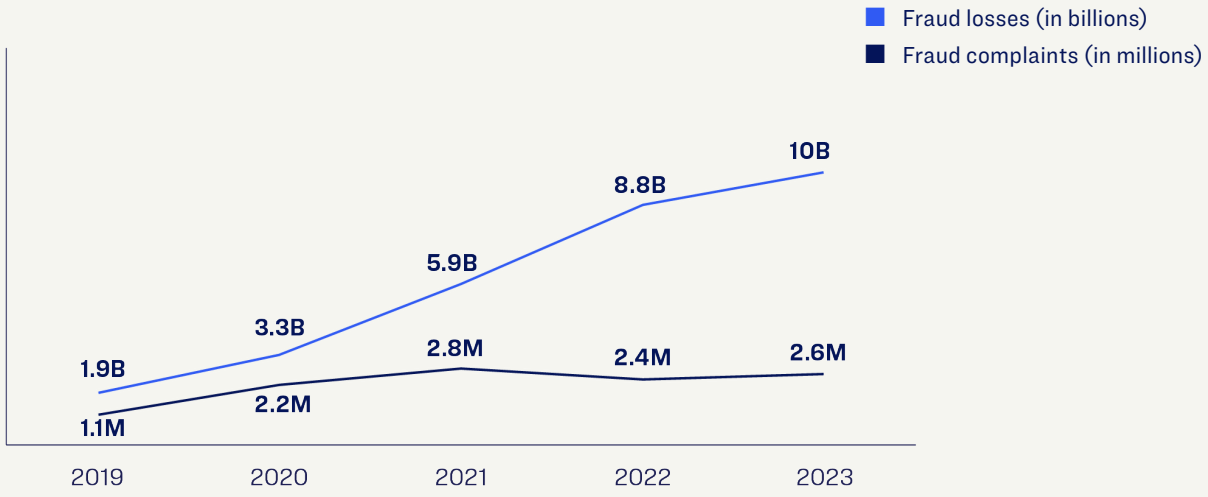
"Retirement plan providers must take cybersecurity and fraud seriously. Excellence in cybersecurity and fraud management builds trust with plan participants."

Upendra Mardikar
Chief Information Security Officer, TIAA

# Introduction

The landscape of fraud is ever changing. As shown in Figure 1, over the course of the Covid-19 pandemic fraud complaints doubled while total reported losses rose fivefold from $1.9 billion to $10 billion.[15, 16] Technological advances in artificial intelligence, telecommunications and social media have made it simple and cost-effective for transnational crime syndicates to target people across the world with alarming speed and sophistication. Adding to the problem, the anonymity and lack of regulation in cryptocurrencies have amplified the magnitude of fraud losses and provided an efficient means for cybercriminals to launder stolen funds.[17, 18]

**FIGURE 1. FRAUD COMPLAINTS AND REPORTED LOSSES FROM 2019–2023**




Source: FTC Consumer Sentinel Network Data Books from 2020 – 2024 (5 consecutive reports).
https://www.ftc.gov/enforcement/consumer-sentinel-network/reports

The global scale of fraud presents a considerable threat to targeted victims and criminal justice advocates. U.S. law enforcement agencies are limited in their ability to identify, detain, and prosecute overseas criminals, and financial institutions are often unsuccessful in recovering funds that have been transferred internationally.[19] As a result, organized crime syndicates—including state-sponsored criminals—have amassed substantial capital. This allows them to invest in the latest technological infrastructure to develop and execute more sophisticated scams using resources like call centers, mobile app and website developers, attractive models (for romance scams), human resource departments, and marketing teams.[20]

"Today's scams are more coordinated, more sophisticated and more personalized."

Ray Bellucci
EVP, Head of Recordkeeping and RK Strategy and Transformation, TIAA

Scammers also use artificial intelligence (AI) to enhance their deceptions. For example, generative AI allows scammers to draft persuasive messages with perfect grammar and punctuation. Recent news reports chronicle the alarming use of deepfake technology to digitally clone the voices and likenesses of victims' relatives, coworkers and even celebrities, deceiving victims into transferring substantial funds.[21] Criminals can also use AI to conduct research on and create profiles of potential targets en masse, saving them time and equipping them with personal details to use in more targeted attacks. These technological tools have alarmed officials because AI-enhanced scams are much harder for consumers to identify as fake, especially consumers who are less familiar with the capabilities of generative AI.[22, 23]

## Common scams affecting older adults

A vast taxonomy of scams vary in prevalence and severity,[24] but several forms—and their variations—have a disproportionate impact on older adults. A prime example is imposter scams that use a wide range of deceptive tactics to convince targets the scammer is a family member or friend, a representative with a well-known business or organization (e.g., a bank), or a government agent. More than 850,000 instances of imposter scams were reported by the FTC in 2023.[25] Scammers adopt fake personas to exploit a potential target's willingness to comply with requests from government agencies and companies they trust.

In a family/friend imposter scam, a person may be led to believe a relative is in trouble and the fastest way to help them is to buy gift cards or send cryptocurrency. In a government imposter scam, criminals may pretend to be with the Internal Revenue Service (IRS), claiming the target owes back taxes and will face jail time if they don't pay immediately. Or they may pretend to be an agent with the Social Security Administration, informing the target their identity is being used to commit serious crimes. Scammers use low-cost tools such as number spoofing and Voice over Internet Protocol (VoIP) to make it appear as though their calls are coming from the impersonated agency or company rather than an overseas call center.

### Key scam types


Investment scams


Romance scams


Business imposter


Government imposter


Prize, lottery, sweepstakes

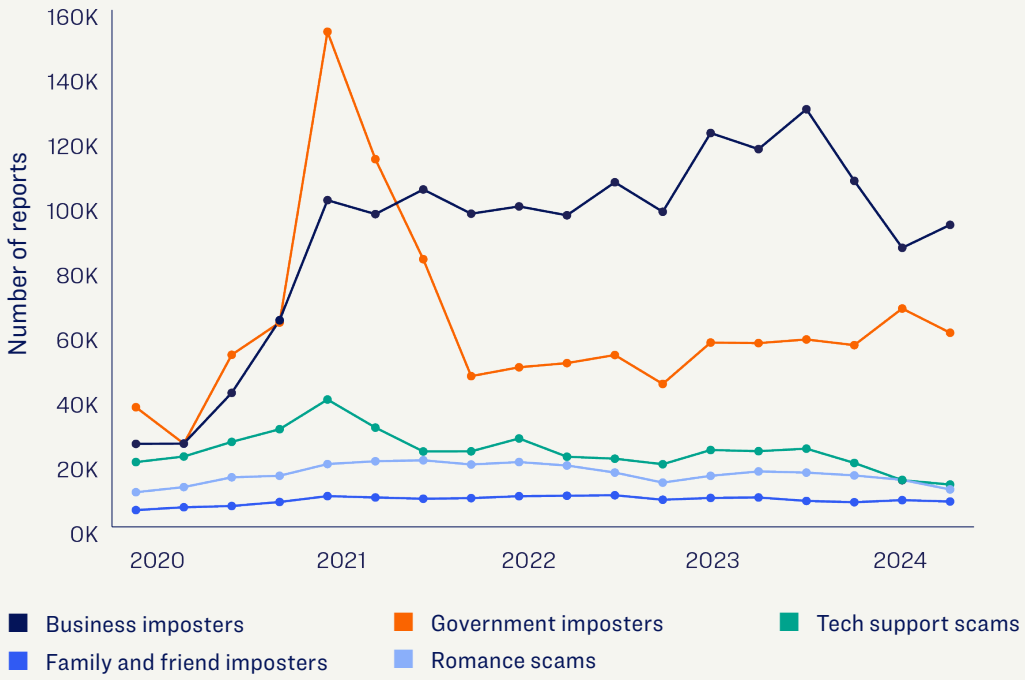

Family/friend imposter

"Technologies today provide the ability for anyone to convincingly portray themselves as someone or something else."

Rick Swenson
Managing Director, Fraud Strategy & Governance, TIAA

Figure 2 shows how the reported prevalence of different types of imposter scams has changed over time. Before the Covid-19 pandemic, government imposter scams were the most prevalent frauds in the United States,[26] but during lockdown criminals quickly pivoted to impersonating entities consumers were depending on for purchasing goods and accessing services, such as online retailers, software companies and shipping companies.[27] In the tech support imposter scam, for example, scammers convince their targets to grant them remote access to their computers, whereby they can view account balances, steal identifying information, and install malware. Based on reports to the FTC, older adults were over six times more likely than younger people to report losing money on a tech support scam in 2022.[28]

**FIGURE 2. DIFFERENT TYPES OF IMPOSTER SCAMS OVER TIME**




Source: FTC's Consumer Complaint Database using Tableau. The Big View: All Sentinel Reports, Federal Trade Commission, published July 24, 2024. https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports.

Imposter scams are still evolving. Instead of impersonating just one entity, criminals are adopting multiple identities within the same interaction with a target. In these hybrid imposter scams, the criminal might pretend to be calling from a tech support company, but once they find a "problem" with the target's online bank account, they'll dial-in a fake bank representative who will confirm there has been fraudulent activity related their accounts. Then they'll connect them to a fake FBI agent who will supposedly investigate the case and help the target move their money to a "secure account."[29] These multiple handoffs help establish credibility and the perceived seriousness of the issue, putting more pressure on the target to comply.

"Get rich quick" schemes are another category of scams affecting older Americans. Investment scams are associated with some of the largest personal losses.[30] According to fraud complaints to the FBI, investment fraud losses rose 38% from $3.3 billion in 2022 to $4.6 billion in 2023.[31] Research indicates older males with investable assets are the most likely to be targeted.[32] Investment scams have also evolved to capitalize on the excitement around cryptocurrencies. False claims about profitable cryptocurrency investments have caused significant harm to thousands of investors who discover their money was stolen and never invested at all.

Criminals may also impersonate a sweepstakes organization or a foreign lottery. They inform the target they're already a winner but first must pay the taxes or a transport fee to receive the cash prize.

Of all deceptive schemes, online romance scams may cause the greatest harm to older victims. Lured by promises of love and companionship, victims are groomed by remote predators for months as they establish a confidential and hyperpersonal relationship. In time, the fake love interest presents a series of fabricated crises that are keeping them apart—an unexpected hospitalization, a business deal gone bad, loss of employment, a theft, travel issues and other problems. They ask the victim for financial help to resolve each crisis so they can finally be together.[33] Using consumer complaint data from the FTC, DeLiema and Witt (2023) found that median losses were $10,000 for those aged 70 and older and ranged from $450 to $3,000 for consumers younger than age 50.[34] Not only are these scams costly—with some victims liquidating their retirement accounts and borrowing money from friends and family to send to the scammer[35]—they also have severe emotional consequences.[36] A qualitative study found some victims described the emotional fallout as being worse than the financial losses that wiped out their savings.[37]

## Persuasion tactics used to manipulate older adults

Scammers use social engineering to manipulate their targets to send them money through various transfer mechanisms, such as by purchasing gift cards and reading the activation codes over the phone, transferring funds from a bank account, using peer-to-peer money transfer apps, wiring funds, providing credit card information, and converting cash into cryptocurrency using a cryptocurrency ATM. While the premises of popular scams and preferred methods of money transfer are constantly changing, scammers' main persuasion tactics have remained consistent.

"The easiest way for scammers to get the money is to have the client move it themselves."

Dale Jones
Managing Director and Head of Enterprise Fraud Management, TIAA

### Authority

One of scammers' most common persuasion tactics is authority. In impersonation schemes they may create fake job titles and pretend to be affiliated with recognizable and trusted organizations. They may say they are an FBI agent, a police officer, a computer repair technician, a fraud investigator or a registered investment advisor. According to Robert Cialdini (2021), a leading expert on social influence, this tactic works because people tend to follow the lead and advice of credible, knowledgeable experts.[38] The use of authority activates decision-making shortcuts in processing new information: authority = expert = trustworthy. This mental shortcut prevents people from critically analyzing the information they're being told.

### Emotional arousal

Scammers also use tactics to elicit powerful emotions. Depending on the type of scam, these include high-arousal positive emotions like excitement, surprise, and exhilaration, as well as high-arousal negative emotions like anger and fear. By their very nature, high-arousal emotions consume cognitive resources and motivate individuals to act immediately based on instinct rather than reasoned analysis.[39] In a highly emotional state, people tend to process scam messages more superficially and miss the red flags that are detected by paying close attention.[40] In one study, Wang and colleagues (2012) found that attention to emotional triggers in a phishing email reduced the cognitive effort spent processing the message, decreased attention to the deception cues in the message, and increased the likelihood of responding.[41] Kircanski and colleagues (2018) found when older adults were made to feel excited or frustrated in a research setting and then shown deceptive advertisements, they were more likely to say they'd be willing to purchase the falsely advertised items compared to participants in a calm emotional state.[42]

### Urgency or scarcity

Scammers put intense pressure on their targets to act quickly. They might claim, "If you don't transfer funds now, the government will seize your assets!" Even positive solicitations can evoke a sense of urgency, such as "Invest

now! This opportunity won't last!" These manipulations are effective for three reasons. First, they produce an emotional response that impairs rational thinking. Second, when people are put under pressure, they feel they have less time to ask critical questions and seek a second opinion. Third, according to the scarcity principle, when people think they'll lose out on something because it is limited or temporary—whether it's a prize, investment offer or discount on a product—they tend to want it more.[43]

### Secrecy

Scammers know their fake stories and manipulations will unravel if the target talks to someone they know and trust before sending money. To keep the target under their influence, scammers will tell them to keep all interactions private and confidential. Some scammers use threats to enforce secrecy. In virtual kidnapping scams, for example, targets may be told their family member will be harmed if they go to the police. In a lottery scam, the target may be told not to talk about their winnings because then everyone will come asking for money. To avoid intervention from outside parties, scammers may even craft lies for the target to use if they're questioned about the purpose of a financial transaction. They coach them to tell lies—such as they are buying gift cards for a grandchild's birthday or cashing out their investments to pay for a home remodel.

### Phantom fixation

Many scams are specifically tailored to respond to targets' unmet needs. These needs may include a desire for companionship, romance, financial independence, respect or even a sense of purpose. Once a scammer identifies these unmet needs in their target, they will use phantom fixation to activate the target's desire and deepen their commitment to the scam's premise.[44, 45] For example, romance scammers send frequent text messages to their targets describing a romantic future together.[46] Investment scammers will promise financial freedom and activate fantasies of wealth and luxury.[47] This visceral imagery helps the target envision a more desirable future—one they're told can only be achieved by complying with the scammer's demands.

These persuasion tactics are only a sampling of the many manipulation tools in a scammer's arsenal. They also vary based on the type of scam. Consumers should familiarize themselves with these tactics, and if they're detected in any communication context, take it as a signal to exit the interaction and talk with someone they know and trust.

### Key persuasion tactics

- Authority
- Emotional arousal
- Urgency or scarcity
- Secrecy
- Phantom fixation

## Age-associated risk factors

Research on the relationship between scam susceptibility and aging presents a mixed picture.[48] Some studies suggest young and middle-aged adults are more likely to be victims than older adults.[49, 50, 51] However, these studies rely on people to self-report scam victimization, and older adults may be less likely to disclose victimization when asked in a survey.

A growing number of studies indicate that age-associated risk factors, such as cognitive impairment and social isolation, are associated with greater scam susceptibility.[52] Declines in cognitive functioning and, more specifically, declines in executive functioning, are the most cited risk factors for scam victimization in older adults. Executive functioning includes higher-level cognitive skills like critical reasoning, working memory, self-control, planning and organization. These cognitive skills are critical for making sound financial decisions and resisting persuasion attempts. Poor executive functioning, challenges with working memory and even mild cognitive impairment have been associated with greater susceptibility to scams in prior research.[53–58]

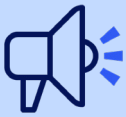
Rates of social isolation and loneliness are high among older Americans.[59] Social isolation refers to the level and frequency of one's social interactions, whereas loneliness is the subjective feeling of being isolated and lacking companionship. These two factors are independently associated with fraud victimization. Research by the FINRA Investor Education Foundation, Stanford University, and the Better Business Bureau shows that when people engage

with a scammer or fraudulent offer, they're more likely to be victimized if they don't have anyone to discuss it with.[60] Single, divorced and widowed survey respondents were more likely to indicate no one was available to talk to about the scam compared to married respondents and those living with a partner.[61] In other words, being alone or socially isolated when exposed to scams can make a person more vulnerable.

Numerous studies have also shown that loneliness and psychological vulnerability are also associated with victimization.[62, 63, 64] Scam messages are intentionally designed to exploit psychological vulnerabilities and unmet needs,[65] and lonely individuals may be more willing to engage with scammers who provide emotional validation and companionship. The prevalence of loneliness among older adults increased during the Covid-19 pandemic,[66] corresponding to a rise in online romance scams.[67] Prior to the pandemic in 2018, a University of Michigan poll found that 27% of adults aged 50 to 80 reported feeling isolated some of the time or often.[68] This increased to 56% during the pandemic, and although rates have fallen to 34%, loneliness is still higher than prepandemic levels.

Major life events such as retirement, widowhood, divorce and onset of disability, may also increase victimization risk because they create psychological or financial need states. A series of national fraud prevalence studies from the FTC

Scam messages are intentionally designed to exploit psychological vulnerabilities and unmet needs.



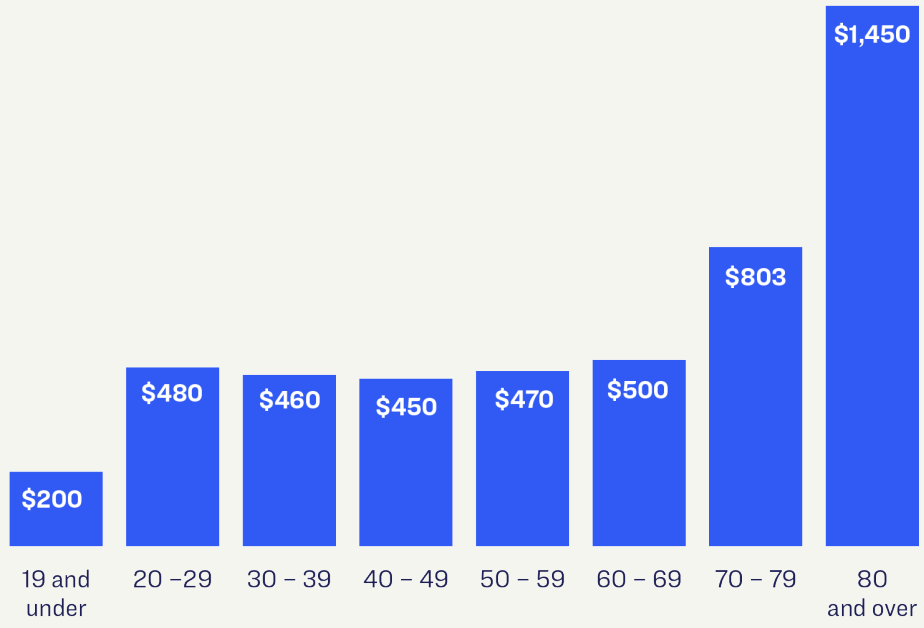
have all indicated victims report a higher number of negative life events in the prior two years relative to nonvictims.[69, 70] Qualitative interviews with individuals who experienced scams also suggest that significant negative life events were a precursor to victimization for many people.[71] Lastly, after a lifetime of earning and saving for retirement, older adults have amassed more assets than young and middle-aged adults, on average.[72] This makes them more attractive targets to financial predators. It is important to note, however, that people experience varying health, social and financial trajectories as they age, so risk factors like cognitive decline, loneliness and wealth accumulation aren't universal among the older population. In fact, young adults who have these characteristics may be equally vulnerable to exploitation.

## Costs and consequences of victimization

Most scams are never reported to authorities. For example, Raval (2020) found that for fraud cases involving low dollar losses—under $100—fewer than one in 1,000 victims file a complaint.[73] Complaint rates increase considerably when losses are greater. Nonetheless, this variation makes it difficult to estimate the true prevalence and cost of victimization among older adults. AARP projects that, as a group, older Americans have $8 billion stolen by scammers each year,[74] whereas the FTC—using different assumptions on the extent of underreporting and average losses per scam—estimates older adults have somewhere between $5.9 billion and $48.4 billion stolen by scammers each year.[75]

Older adults report higher median losses per scam than their younger counterparts. As shown in Figure 3, median fraud losses among adults ages 80+ were three times higher than median losses among those younger than age 60 in 2023 ($1,450 versus $450–$480).[76]

**FIGURE 3. MEDIAN FRAUD LOSS BY AGE**




Source: Consumer Sentinel Network Data Book 2023, Federal Trade Commission, published Feb., 2024. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023.

In addition to the Federal Trade Commission, many victims report fraud directly to the FBI. Fraud complaints submitted to the FBI's reporting center—the Internet Crime Complaint Center (IC3)—paint an even starker picture of personal losses experienced by older Americans. Average losses among adults ages 60+ were nearly $34,000. This is quadruple the average loss amount reported to the FBI just three years earlier in 2020 ($9,175).[77, 78] These trends suggest criminal enterprises are becoming more successful at extracting significant amounts of money from older people.

Using data from the national Health and Retirement Study, DeLiema and colleagues (2017) found that fraud victimization among those age 50+ was linked to a decline in nonhousing wealth.[79] Having retirement savings stolen by scammers can lead to dependence on friends and family members, and in extreme circumstances, reliance on government programs designed to support low-income Americans. A 2016 study focusing on New York State estimated elder financial exploitation costs the public $6.2 million per year for investigation and response, plus an additional $8.3 million in expenditures on public benefits to financially support victims who had their resources stolen.[80]

In addition to monetary losses, the nontraditional costs of scam victimization can be severe.[81] Additional outcomes may include job loss, legal problems, divorce, severe emotional distress, and prolonged indebtedness.[82–86] Physical health outcomes include increased blood pressure among male victims[87] and poor sleep.[88] Research has also identified persistent mental health problems, including anxiety, depression, trauma, and suicidality, but several of these studies weren't focused specifically on older adults.[89–94]

People who experience victimization are often blamed for being too gullible, trusting and foolish, and may be dismissed by police, who sometimes perceive them as actively having contributed to their own victimization.[95] As a result, victims may feel ashamed and blame themselves, which further discourages help-seeking[96] and reduces confidence in financial matters.[97]

# Fraud prevention and intervention

As with preventing and managing a chronic disease, protecting older adults from scams requires primary, secondary and tertiary prevention.

Primary prevention focuses on reducing the risk of exposure to and engagement with scams. Secondary prevention (intervention) refers to responding to immediate threats and protecting funds if scam victimization is suspected or has occurred. Tertiary prevention aims to reduce the longer-term risks and harm associated with scam victimization.

### Primary prevention

- Enhance scam awareness
- Reduce social isolation and loneliness
- Activate online and mobile accounts
- Opt-in to account security features
- Engage in advance financial care planning
- Name a trusted contact or every retirement and investment account

### Secondary prevention

- Investigate suspicious activity and behavior
- Ask questions and educate plan participants on fraud risks
- Secure accounts through temporary holds
- Report fraud to law enforcement
- Recover funds
- Refer to victim support services

### Tertiary prevention

- Engage trusted contact
- Involve agents under power of attorney to provide support and financial oversight
- Monitor financial accounts
- Address unmet needs (e.g., financial security, social interaction, sense of purpose)
- Referrals to legal, financial, and mental health services

## Primary prevention: reducing risk of exposure to and engagement with scams

**Scam awareness and consumer education**

The most effective way to minimize the impact of victimization is to prevent scam exposure and fortify a person's defenses. Raising awareness about common scams and persuasion tactics is a key component of primary prevention. The FTC recently convened a panel of experts to survey the literature on effective consumer fraud education and scam awareness messaging for older adults.[98] Their review indicates scam awareness messages should be memorable and action-oriented, use empowering language (no victim blaming) and focus on the positive benefits of heeding the message. Specific action steps might include advice on hanging up on unknown callers, refusing to allow strangers to remotely access your computer, and talking to trusting family members before making any large investments or transactions.

Several studies demonstrate that forewarning vulnerable older adults about scams significantly reduces their likelihood of becoming a victim.[99, 100, 101] DeLiema, Yi, and Mottola (2023) found that individuals who had heard about a particular scam prior to being targeted by that scam were nearly half as likely to lose money compared to those who were unfamiliar.[102] A research study led by Jeremy Burke (2022) found that participants who received text or video education on investment scams were significantly less likely to express a willingness to invest in fraudulent investment opportunities than individuals who received no training.[103] These and other studies suggest prior knowledge about specific scams confers protection, but fraud awareness campaigns may struggle to keep pace with evolving schemes. Moreover, evidence suggests consumers forget fraud-protection tips over time.[104, 105] To reduce the decay in fraud knowledge, reminder messages should be sent a minimum of every few months.[106, 107] These "booster" messages need to be updated to include information on how scams have evolved and what new red flags to pay attention to.

"Now that scammers use generative AI, we need to throw out all our old consumer advice. For example, we can't tell people to pay attention to spelling errors anymore because messages are written by AI with perfect grammar."

Brendan Purcell
Senior Director, Enterprise Fraud Detection, TIAA

Relative to young adults, older adults tend to process and recall positively framed messages better than negatively framed messages.[108] In a recent intervention study to reduce repeat mail fraud victimization, Langton and colleagues (2024) found older victims who received a series of empowering "Be a Fraud Fighter" letters, brochures, and newsletters were less likely to lose money in a subsequent mail scam than older victims in the control group who didn't receive any fraud fighter materials in the mail.[109] Similar messaging can be adapted for distribution through digital and text message channels.

One challenge for effective consumer education campaigns is that individuals suffer from "optimism bias" and discount their personal susceptibility to scams.[110] This reduces their attention to and recall of fraud prevention messages. To overcome optimism bias, scam awareness messaging should be memorable and personally relevant,[111] and it should use compelling stories to help people connect with the experience of victimization. For example, some studies have simulated the experience of being scammed using mock email phishing attacks.[112] This makes the red flags and warning messages more memorable.

**Educating financial advisors and plan sponsors**

Educating financial advisors on the red flags of fraud is critical. Advisors may work with the same plan participants for decades and through multiple life stages. They often notice early changes in their plan participant's behavior or risk preferences that could signal diminished financial capacity—a risk factor for fraud. Financial advisors should carefully document their conversations with plan participants, follow up with a phone call or email, and contact the plan participant's trusted contact if they have concerns.[113]

In addition to educating retired plan participants and financial advisors about fraud, companies must educate plan sponsors and their employees. Imparting participants with a watchful mindset may well carry over and provide them a measure of protection once retired. A layered approach to fraud prevention education is optimal because it helps reach people across the lifespan and protects businesses from social engineering attacks targeting employees.

**Activating account safeguards**

Financial institutions that prioritize plan participant safety invest in the latest tools and technologies to monitor and protect their accounts from unauthorized access, identity theft, and fraud. A core component of account security is verifying plan participants' identities and making sure they're not being manipulated to act against their best financial interests. Strategies may include using advanced machine learning, behavioral biometrics and AI-detection to identify unusual account activity or behaviors that are inconsistent with a plan participant's past activity, device use or location. These enhanced fraud-detection tools help indicate whether the plan participant is experiencing a scam or if an unauthorized third-party is attempting to access their accounts.

Plan participants also play a proactive role in keeping their retirement accounts secure by engaging in fraud prevention measures.

## Fraud prevention measures

- Activate mobile and online accounts and monitor those accounts
- Keep contact information on accounts up to date
- Use multifactor authentication
- Enroll in push notifications to receive account activity updates in real time
- Leverage mobile phone biometrics
- Choose complicated and unique passwords and store them securely

In addition to activating security features on online accounts, reducing exposure to Internet-enabled scams requires protecting devices from theft and malware. Plan participants should use virus protection software, install pop-up blockers on their web browsers, and update and install security patches when prompted.

To overcome issues related to poor password security, many companies are leveraging passkey-enabled authentication, whereby a digital credential is tied to the plan participant's account. Passkeys are more resistant to theft and phishing attacks than traditional passwords because they rely on a person's unique biometric signature—e.g., face scan or fingerprints—to access online accounts.

"We can win against bad actors. We all need to engage our understanding of their threats, educate ourselves on their tactics, and empower ourselves to defeat them."

Ron Barthel
Senior Director, Global Cybersecurity & Fraud Management, TIAA

In addition to maintaining the security of financial accounts, all social media users should understand the risks of accepting new friends or follow requests from people they meet on the Internet. Plan participants should also be aware that scammers can "spoof" caller IDs and make it appear as if they're calling from a legitimate organization or government agency rather than a scam call center across the globe. Consumer education should include advice about never engaging in remote financial transactions with social media contacts or callers on the telephone.

**Advance financial care planning**

As people age they may experience health challenges that make managing their accounts and making financial decisions more difficult. This can increase their risk of scams and fraud. To keep their retirement accounts safe as they age, plan participants should engage in advance financial care planning. This involves making sure beneficiary designations are up to date, appointing trustworthy and dependable agent(s) under power of attorney (POA), and designating a trusted contact for their retirement and investment accounts.

### Advance financial care planning strategies

Trusted contact

Power of attorney

Revocable or irrevocable trust

All plan participants should complete the trusted contact form provided by their retirement plan company. This form authorizes the retirement plan company to contact the named person under specific circumstances, such as if they can't reach the plan participant or are concerned about the plan participant's financial well-being due to suspicious account activity or behavior. Like naming an emergency contact before engaging in risky physical activities, having a trusted contact on file adds an additional layer of protection against scams. This person isn't authorized to see the plan participants' account information or transact any business; however, they can confirm the person's contact information and health status, and help the retirement plan company connect with someone authorized to access the plan participant's accounts.

Naming a trusted contact provides an additional layer of protection against scams.

An important retirement safeguard is to appoint a trusted friend or family member to act as an agent under power of attorney (POA). This legal process authorizes the appointed person (or multiple people) to make financial decisions on the plan participant's behalf. Plan participants can decide what financial "powers" their agent is authorized to carry out. For example, the agent can be empowered to assist with the plan participant's investment and disbursement decisions and monitor their accounts for suspicious behavior or activity. Having an agent under POA is like having an extra set of eyes and ears to guard against scams and account takeovers, but it's critical the appointed agent is trustworthy and reliable, makes good financial decisions, understands the financial goals of the plan participant, and always acts with integrity.

## Secondary prevention: intervention

Scams are becoming increasingly sophisticated, so when prevention fails, it's important to have a second line of defense. Secondary prevention includes in-the-moment scam warnings, counseling plan participants who are believed to be experiencing fraud to disengage with the scam, slowing down transactions, and reporting stolen funds as soon as possible.

**In-the-moment warnings**
If suspicious account activity is detected, financial institutions can warn plan participants with mobile and email push notifications. To receive timely alerts, plan participants should make sure their contact information is up to date and they have mobile and online accounts activated. If they receive a push notification about a transaction they didn't authorize, plan participants should immediately call their financial institution to confirm it was fraud.

Push notifications and other in-the-moment warnings have the potential to stop fraud in its tracks, but only if the plan participant pays attention to the message. Criminals use fear, excitement, urgency and other emotional arousal tactics to distract plan participants from processing warning messages.[114, 115] They also coach them to ignore consumer education and give false justifications for the purpose of a transaction. In these situations, it's the plan participant moving money out of their account, not a cybercriminal who's taken over their account without their knowledge.

Push notifications about suspicious activity may not be effective when the plan participant is being manipulated to authorize the transaction. Instead, retirement plan providers may ask for additional verification from the plan participant in the notification message to slow down the process, such as requiring them to speak to a representative over the phone before they can proceed.

"You can't just look at the transaction. You need to know who wants it and why."

Rick Swenson
Managing Director, Fraud Strategy & Governance, TIAA

**Communicating with plan participants experiencing scams**
Financial institutions that value client protection train their investment advisors and other client-facing employees to detect if a plan participant is being coached by a scammer and motivate them to end the interaction and report to authorities. When intervening, it's important for financial professionals to be patient when describing their concerns and asking key questions about the intended purpose of a suspicious transaction or request. Nonaccusatory, empathetic communication is essential to build trust. The goal is to make plan participants feel safe disclosing truthful information about a transaction they were instructed to keep as a secret or lie about. Because financial predators use undue influence to control their victims, intervenors need to anticipate they may be met with denial, frustration and even lies. It's critical to be persistent with plan participants and be willing to temporarily suspend transactions while investigations take place but also clearly communicate the purpose of the hold to plan participants and inform them right away.

"You need to train employees to have conversations in an entirely new way. They can't just read off a checklist and ask 'yes' or 'no' questions. Empower them to ask deeper questions and engage the client in a dialogue."

Brendan Purcell
Senior Director, Enterprise Fraud Detection, TIAA

**Reporting scam victimization**
Notifying authorities about scam victimization is critical for several reasons. For one, reporting a financial loss within 24 hours of the fraudulent transaction increases the likelihood of recovering stolen funds. Second, reporting to local and federal authorities allows law enforcement to investigate the crime and pursue justice against the perpetrators.

Plan participants should start by contacting their financial institutions to notify them about the scam and state which transactions were fraudulent. Banks and investment companies may be able to reverse these transactions or contact the receiving institution to hold the funds before the perpetrators withdraw money. Next, plan participants should report fraud to the Federal Trade Commission, FBI and local law enforcement. While these agencies may not investigate individual cases, reports help them identify patterns in scam victimization and build cases against the large criminal networks involved in fraud and their domestic co-conspirators who launder stolen funds. If future actions result in a financial settlement, reporting helps entitle plan participants to recovered funds.

More than half of U.S. states mandate that financial institutions report suspected elder financial exploitation and fraud to local adult protective services[116] (APS). APS workers are trained to interview the older person and assess their level of risk and need for assistance, such as oversight from family or friends, nutrition services, and safer housing. APS may cross-report to local law enforcement to further investigate allegations. It's important for financial professionals to be familiar with their reporting requirements and protocols for sharing plan participant information with law enforcement and APS. Interagency collaboration is essential for addressing complex cases and supporting vulnerable adults.

### Tertiary prevention: protecting plan participants from future scams

Scam victimization is highly stigmatized. It can take time for victims to come to terms with the financial consequences and to rebuild their sense of safety and financial confidence. Unfortunately, while victims are recovering from fraud, they may be bombarded by more deceptive offers because their contact information was added to "lead lists" and sold to other scammers.[117] This places victims at high risk of revictimization. Financial professionals should work with plan participants who have experienced scams to review their accounts, update passwords, opt in to security features, and make sure their POA and trusted contact forms are up to date.

If a financial advisor has concerns about a plan participant's financial capacity, they may reach out to the individual listed as a trusted contact. This person can help by verifying the plan participant's health status and determining if more financial oversight and assistance is needed from friends or family. If a POA is listed on the account, the financial advisor should encourage the plan participant to invite their agent to become more involved with money management and investment decisions, perhaps by inviting everyone to gather for a retirement plan review meeting.

Respecting a plan participant's financial autonomy and desire for privacy is paramount, but safety and financial well-being are also top priorities. Financial institutions have an obligation to prevent fraud and not to facilitate suspected criminal activity. In cases where plan participants are unable to recognize they're being victimized and are at risk of authorizing further fraudulent transactions, retirement plan providers can place temporary holds on the disbursement of funds from their accounts. Before placing a temporary hold on funds, the company must have a reasonable suspicion the plan participant is experiencing a scam or is being exploited by a friend or family member. Temporary holds give the company time to investigate suspicious activity and share concerns with law enforcement, APS, federal and state regulators, as well as notify trusted contacts and agents under POA. In challenging cases, financial institutions should be prepared to work closely with law enforcement and APS to prevent repeat victimization—such as through regular account activity monitoring—and address the plan participant's underlying health and safety needs.

Reducing a plan participant's risk of revictimization requires addressing the underlying need states that drove them to respond to the scam solicitation in the first place. Financial and emotional need states may be caused by financial insecurity, loss of purpose, bereavement and social isolation. Addressing these needs among older adults is an important role for family members, friends, neighbors, social service agencies and the broader community. Financial institutions and plan sponsors can help by engaging in scam awareness outreach, educating employees, and advocating for programs that support people as they age.

## Conclusion

Financial scams are a global problem. Bold new strategies and solutions are needed to pull ahead in the technological race against scammers and cybercriminals. Retirement plan providers must work hand-in-hand with plan sponsors, plan participants and other financial industry partners to defend against these evolving threats to Americans' retirement security. Effective scam prevention will also require building bridges between the financial services industry, the adult protection system and the criminal justice system. By teaming up to fight fraud, Americans have brighter opportunities to achieve their retirement goals.

"If only one company fights fraud individually, we won't be successful. We need a unified front. We need to share tools."

Upendra Mardikar
Chief Information Security Officer, TIAA

# Endnotes


1 Federal Trade Commission (2024). Consumer Sentinel Network Data Book, 2023. https://www ftc gov/reports/consumer-sentinel-network-data-book-2023

2 Robinson, J., & Edwards, M. (2024). Fraudsters target the elderly: Behavioural evidence from randomised controlled scam-baiting experiments. *Security Journal,* 1–24.

3 DeLiema, M., Langton, L., Brannock, D., & Preble, E. (2024). Fraud victimization across the lifespan: evidence on repeat victimization using perpetrator data. *Journal of Elder Abuse & Neglect*, 36(3), 227–250.

4 Xin, Y., Xia, Y., & Chai, Y. (2024). Routine activities and fraud re-victimization among older adults: Do types of routine activities matter? *Criminology & Criminal Justice*, https://doi.org/10.1177/17488958241257860

5 Burnes, D., Henderson Jr, C. R., Sheppard, C., Zhao, R., Pillemer, K., & Lachs, M. S. (2017). Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis. *American Journal of Public Health*, 107(8), e13–e21.

6 Beals, M. E., Carr, D. C., Mottola, G. R., Deevy, M. J., & Carstensen, L. L. (2017). How does survey context impact self-reported fraud victimization? *Gerontologist*, 57(2), 329–340.

7 Raval, D. (2020). Whose voice do we hear in the marketplace? Evidence from consumer complaining behavior. *Marketing Science*, *39*(1), 168–187. doi:10.1287/mksc.2018.1140

8 Federal Trade Commission (2024) Consumer Sentinel Network Data Book, 2023. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2019

9 Cross, C., (2018). (Mis)understanding the impact of online fraud: Implications for victim assistance schemes. *Victims & Offenders*, 13(6), 757–776.

10 Cross, C. (2019). "You're not alone": The use of peer support groups for fraud victims. *Journal of Human Behavior in the Social Environment*, 29(5), 672–691.

11 Jackson, S. L., (2021). Recognizing the trauma experienced by community-dwelling older victims of financial abuse perpetrated by trusted others. In *Handbook of Interpersonal Violence and Abuse Across the Lifespan* (pp. 4499–4518). Springer International Publishing

12 DeLiema, M., Volker, J., & Worley, A. (2023). Consumer experiences with gift card payment scams: Causes, consequences, and implications for consumer protection. *Victims & Offenders*, 18(7), 1282–1310.

13 Mighdoll, P. (2003). Prosecuting crimes against the elderly while addressing the victim's loss of autonomy. *Marquette Elder's Advisor*, *5*, 129–135.

14 Parti, K., & Tahir, F. (2023). "If We Don't Listen to Them, We Make Them Lose More than Money:" Exploring Reasons for Underreporting and the Needs of Older Scam Victims. *Social Sciences*, *12*(5), 264.

15 Federal Trade Commission (2020). Consumer Sentinel Network Data Book, 2019. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2019

16 Federal Trade Commission (2024) Consumer Sentinel Network Data Book, 2023. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023

17 Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*, 1–35.

18 Wronka, C. (2022). "Cyber-laundering": The change of money laundering in the digital age. *Journal of Money Laundering Control*, *25*(2), 330–344.

19 Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, 20(3), 358-375.

20 Wang, F., & Topalli, V. (2024). The cyber-industrialization of catfishing and romance fraud. *Computers in Human Behavior*, 154, 108133.

21 Flitter, E., & Cowley, S. (2023, August 30). Voice deepfakes are coming for your bank balance. *New York Times*. https://www.nytimes.com/2023/08/30/business/voice-deepfakes-bank-scams.html

22 King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics, 26*, 89–120.

23 U.S. White House (2023). Fact sheet: President Biden issues executive order on safe, secure, and trustworthy artificial intelligence. White House Press Release. https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

24 Beals, M., DeLiema, M., & Deevy, M. (2015). Framework for a taxonomy of fraud. Financial Fraud Research Center. https://wayback.stanford.edu/was/20220430052639mp_/http://longevity3.stanford.edu/wp-content/uploads/2015/11/Full-Taxonomy-report.pdf

25 Federal Trade Commission (2024) "Impersonation scams: not what they used to be." Consumer Protection Data Spotlight. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/04/impersonation-scams-not-what-they-used-be

26 Federal Trade Commission (2019). "Government imposter scams top the list of reported frauds." Consumer Protection Data Spotlight. https://www.ftc.gov/system/files/attachments/blog_posts/Government%20imposter%20scams%20top%20the%20list%20of%20reported%20frauds/govimposters_spotlight_july2019.pdf

27 Fletcher, E. (2021). Amazon tops list of impersonated businesses. Consumer Protection Data Spotlight. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/10/amazon-tops-list-impersonated-businesses

28 Federal Trade Commission (2023). *Protecting older consumers 2022-2023: A report of the Federal Trade Commission*. https://www.ftc.gov/reports/protecting-older-consumers-2022-2023-report-federal-trade-commission

29 Puig, A. (2024). FTC Data Spotlight: New insights about imposter scams. Available at https://consumer.ftc.gov/consumer-alerts/2024/03/ftc-data-spotlight-new-insights-about-imposter-scams

30 Glodstein, D., Glodstein, S. L., & Fornaro, J. (2010). Fraud trauma syndrome: The victims of the Bernard Madoff scandal. *Journal of Forensic Studies in Accounting & Business*, *2*(1).

31 Internet Crime Complaint Center (2023). Elder Fraud Report 2023. Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf

32 DeLiema, M., Shadel, D., & Pak, K. (2020). Profiling victims of investment fraud: Mindsets and risky behaviors. J*ournal of Consumer Research*, 46(5), 904–914.

33 Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, *53*(4), 665–684.

34 DeLiema, M., & Witt, P. (2023). Profiling consumers who reported mass marketing scams: Demographic characteristics and emotional sentiments associated with victimization. *Security Journal*, 1–44.

35 Schmall, E. (2023, Feb). Retirees are losing their life savings to romance scams: Here's what to know. *New York Times*. https://www.nytimes.com/2023/02/03/business/retiree-romance-scams.html

36 Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, *53*(4), 665–684.

37 Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims—both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176–194.

38 Cialdini, R. (2021). *Influence, new and expanded: The psychology of persuasion*. Harper Collins.

39 Langenderfer, J., & Shrimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory on visceral influences on persuasion. *Psychology & Marketing, 18,* 763–783.

40 Loewenstein, G. (2000). Emotions in economic theory and economic behavior. *The American Economic Review*, *90*, 426–432.

41 Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, *55*, 345–362.

42 Kircanski, K., Notthoff, N., DeLiema, M., Samanez-Larkin, G. R., Shadel, D., Mottola, G., Carstensen, L. L., & Gotlib, I. H. (2018). Emotional arousal may increase susceptibility to fraud in older and younger adults. *Psychology and Aging*, *33*(2), 325.

43 Cialdini, R. (2021). *Influence, new and expanded: The psychology of persuasion*. Harper Collins.

44 DeLiema, M., Shadel, D., & Pak, K. (2020). Profiling victims of investment fraud: Mindsets and risky behaviors. J*ournal of Consumer Research*, 46(5), 904–914.

45 Kieffer, C., & Mottola, G. (2017). *Understanding and combating investment fraud.* In Mitchell, O. S., Hammond, P. B., & Utkus, S. P. (Eds.). *Financial Decision Making and Retirement Security in an Aging World.* Oxford University Press.

46 Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, *53*(4), 665–684.

47 DeLiema, M., Shadel, D., & Pak, K. (2020). Profiling victims of investment fraud: Mindsets and risky behaviors. J*ournal of Consumer Research*, 46(5), 904–914.

48 Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on Psychological Science*, *9*(4), 427–442.

49 Anderson, K. B. (2013). Consumer fraud in the United States, 2011: The third FTC survey. Federal Trade Commission. https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf

50 Anderson, K. B. (2016). Mass-market consumer fraud: Who is most susceptible to becoming a victim? *FTC Bureau of Economics*, (332).

51 Anderson, K. B. (2019). Mass-market consumer fraud in the United States: A 2017 update. Federal Trade Commission. https://www.ftc.gov/es/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf

52 Lachs, M. S., & Han, S. D. (2015). Age-associated financial vulnerability: An emerging public health issue. *Annals of Internal Medicine*, *163*(11), 877–878.

53 Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., ... & Oliveira, D. S. (2020). Uncovering susceptibility risk to online deception in aging. *The Journals of Gerontology: Series B*, 75(3), 522-533.

54 Judges, R. A., Gallant, S. N., Yang, L., & Lee, K. (2017). The role of cognition, personality, and trust in fraud victimization in older adults. *Frontiers in Psychology*, *8*, 588.

55 Lachs, M. S., & Han, S. D. (2015). Age-associated financial vulnerability: An emerging public health issue. *Annals of Internal Medicine*, *163*(11), 877–878.

56 Han, S. D., Boyle, P. A., James, B. D., Yu, L., & Bennett, D. A. (2016). Mild cognitive impairment and susceptibility to scams in old age. *Journal of Alzheimer's Disease*, *49*(3), 845–851.

57 Spreng, R. N., Karlawish, J., & Marson, D. C. (2016). Cognitive, social, and neural determinants of diminished decision-making and financial exploitation risk in aging and dementia: A review and new model. *Journal of Elder Abuse & Neglect*, *28*(4-5), 320–344.

58 Yu, L., Mottola, G., Barnes, L. L., Han, S. D., Wilson, R. S., Bennett, D. A., & Boyle, P. A. (2021). Correlates of susceptibility to scams in community-dwelling older Black adults. *Gerontology*, *67*(6), 729–739.

59 Cudjoe, T. K., Roth, D. L., Szanton, S. L., Wolff, J. L., Boyd, C. M., & Thorpe Jr, R. J. (2020). The epidemiology of social isolation: National health and aging trends study. *The Journals of Gerontology: Series B*, 75(1), 107–113.

60 DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O. S. (2017). Exploring the risks and consequences of elder fraud victimization: Evidence from the Health and Retirement Study. *Michigan Retirement Research Center Research Paper*, (2017-364), 2018-06.

61 DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O. S. (2017). Exploring the risks and consequences of elder fraud victimization: Evidence from the Health and Retirement Study. *Michigan Retirement Research Center Research Paper*, (2017-364), 2018-06

62 DeLiema, M., Li, Y., & Mottola, G. (2023). Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type. *International Journal of Consumer Studies*, 47(3), 1042–1059.

63 Lichtenberg, P. A., Sugarman, M. A., Paulson, D., Ficker, L. J., & Rahman-Filipiak, A. (2016). Psychological and functional vulnerability predicts fraud cases in older adults: Results of a longitudinal study. *Clinical Gerontologist*, *39*(1), 48–63.

64 Wen, X., Xu, L., Wang, J., Gao, Y., Shi, J., Zhao, K., Tao, F., & Qian, X. (2022). Mental states: A key point in scam compliance and warning compliance in real life. *International Journal of Environmental Research and Public Health, 19*(14), e8294.

65 Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*, 231–245.

66 Su, Y., Rao, W., Li, M., Caron, G., D'Arcy, C., & Meng, X. (2022). Prevalence of loneliness and social isolation among older adults during the COVID-19 pandemic: A systematic review and meta-analysis. *International Psychogeriatrics*, *35*(5), 229–241.

67 Buil-Gil, D., & Zeng, Y. (2022). Meeting you was a fake: investigating the increase in romance fraud during COVID-19. *Journal of Financial Crime*, 29(2), 460–475.

68 University of Michigan. National Poll on Healthy Aging (2023). *Trends in Loneliness Among Older Adults from 2018–2023.* https://dx.doi.org/10.7302/7011

69 Anderson, K. B. (2013). Consumer fraud in the United States, 2011: The third FTC survey. Federal Trade Commission. https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf

70 Anderson, K. B. (2019). Mass-market consumer fraud in the United States: A 2017 update. Federal Trade Commission. https://www.ftc.gov/es/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf

71 DeLiema, M., Volker, J., & Worley, A. (2023). Consumer experiences with gift card payment scams: Causes, consequences, and implications for consumer protection. *Victims & Offenders*, 18(7), 1282–1310.

72 Federal Reserve (2024). Distribution of household wealth in the U.S. since 1989 by generation. https://www.federalreserve.gov/releases/z1/dataviz/dfa/distribute/chart/#quarter:138;series:Assets;demographic:generation;population:1,3,5,7;units:levels

73 Raval, D. (2020). Whose voice do we hear in the marketplace? Evidence from consumer complaining behavior. *Marketing Science*, *39*(1), 168–187. doi:10.1287/mksc.2018.1140

74 Gunther, J. (2023). The scope of elder financial exploitations: What it costs victims. AARP Public Policy Institute. https://www.aarp.org/pri/topics/work-finances-retirement/fraud-consumer-protection/scope-elder-financial-exploitation.html

75 Federal Trade Commission (2023). *Protecting older consumers 2022-2023: A report of the Federal Trade Commission*. https://www.ftc.gov/reports/protecting-older-consumers-2022-2023-report-federal-trade-commission

76 Federal Trade Commission. (2024). Reported frauds and losses by age (pp. 13). Consumer Sentinel Network Data Book, 2023. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023

77 Internet Crime Complaint Center (2020). Elder Fraud Report 2020. Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3ElderFraudReport.pdf

78 Internet Crime Complaint Center (2023). Elder Fraud Report 2023. Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf

79 DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O.S.(2017).Exploring the risks and consequences of elder fraud victimization: Evidence from the Health and Retirement Study. *Michigan Retirement Research Center Research Paper*, (2017-364), 2018-06.

80 Huang, Y., & Lawitz, A. (2016). The New York State Cost of Financial Exploitation Study. New York State Office of Children and Family Services. https://ocfs.ny.gov/reports/aps/Cost-of-Financial-Exploitation-Study-2016May.pdf

81 FINRA Investor Education Foundation (2015). *The non-traditional costs of financial fraud.* https://www.finrafoundation.org/files/non-traditional-costs-financial-fraud

82 Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27, 36-54

83 Cross, C., (2018). (Mis)understanding the impact of online fraud: Implications for victim assistance schemes. *Victims & Offenders*, 13(6), 757–776.

84 DeLiema, M., Volker, J., & Worley, A. (2023). Consumer experiences with gift card payment scams: Causes, consequences, and implications for consumer protection. *Victims & Offenders*, 18(7), 1282–1310.

85 FINRA Investor Education Foundation (2015). *The non-traditional costs of financial fraud.* https://www.finrafoundation.org/files/non-traditional-costs-financial-fraud

86 Golladay, K. A., & Snyder, J. A. (2023). Financial fraud victimization: an examination of distress and financial complications. *Journal of Financial Crime*, *30*(6), 1606–1628.

87 Lamar, M., Yu, L., Leurgans, S., Aggarwal, N. T., Wilson, R. S., Han, S. D., Bennett, D. A., & Boyle, P. A. (2022). Self-reported fraud victimization and objectively measured blood pressure: Sex differences in post-fraud cardiovascular health. *Journal of the American Geriatrics Society, 70*(11), 3185–3194.

88 FINRA Investor Education Foundation (2015). *The non-traditional costs of financial fraud.* https://www.finrafoundation.org/files/non-traditional-costs-financial-fraud

89 Acierno, R., Watkins, J., Hernandez-Tejada, M. A., Muzzy, W., Frook, G., Steedley, M., & Anetzberger, G. (2019). Mental health correlates of financial mistreatment in the National Elder Mistreatment Study Wave II. *Journal of Aging and Health*, 31(7), 1196–1211.

90 Cross, C., (2018). (Mis)understanding the impact of online fraud: Implications for victim assistance schemes. *Victims & Offenders*, 13(6), 757–776.

91 Deem, D. L. (2000). Notes from the field: Observations in working with the forgotten victims of personal financial crimes. *Journal of Elder Abuse and Neglect*, 12, 33–48

92 DePrince, A. P., & Jackson, S. L. (2020). Moving the field forward: Elucidating the nexus between elder abuse and trauma. *Journal of Trauma & Dissociation*, 21(2), 151–157.

93 Kemp, S., & Erades Pérez, N. (2023). Consumer fraud against older adults in digital society: Examining victimization and its impact. *International Journal of Environmental Research and Public Health*, *20*(7), 5404.

94 Nguyen, A. L., Mosqueda, L., Windisch, N., Weissberger, G., Axelrod, J., & Han, S. D. (2021). Perceived types, causes, and consequences of financial exploitation: Narratives from older adults. *The Journals of Gerontology: Series B*, *76*(5), 996–1004.

95 Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21(2), 187–204.

96 Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, 518, 1–14.

97 Brenner, L., Meyll, T., Stolper, O., & Walter, A. (2020). Consumer fraud victimization and financial well-being. *Journal of Economic Psychology*, 76, 102243.

98 Federal Trade Commission (2024). A review of scam prevention messaging research: Takeaways and recommendations. Scams Against Older Adults Advisory Group, Scam Prevention Research Committee Report. https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/A%20Review%20of%20Scam%20Prevention%20Messaging%20Research.pdf

99 AARP. (2003). Off the hook: Reducing participation in telemarketing fraud. https://assets.aarp.org/rgcenter/consume/d17812_fraud.pdf

100 Scheibe, S., Notthoff, N., Menkin, J., Ross, L., Shadel, D., Deevy, M., & Carstensen, L. L. (2014). Forewarning reduces fraud susceptibility in vulnerable consumers. *Basic and Applied Social Psychology*, 36(3), 272–279. https://doi.org/10.1080/01973533.2014.903844

101 Burke, J., Kieffer, C., Mottola, G., & Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud? *Journal of Economic Behavior & Organization*, 198, 250–266.

102 DeLiema, M., Li, Y., & Mottola, G. (2023). Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type. *International Journal of Consumer Studies*, 47(3), 1042–1059.

103 Burke, J., Kieffer, C., Mottola, G., & Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud? *Journal of Economic Behavior & Organization*, 198, 250–266.

104 DeLiema, M., Robb, C. A., & Wendel, S. (2024). What does trust have to do with it? Training consumers to detect digital imposter scams. *Journal of Financial Crime*. https://www.emerald.com/insight/content/doi/10.1108/JFC-12-2023-0314/full/html

105 Scheibe, S., Notthoff, N., Menkin, J., Ross, L., Shadel, D., Deevy, M., & Carstensen, L. L. (2014). Forewarning reduces fraud susceptibility in vulnerable consumers. *Basic and Applied Social Psychology*, 36(3), 272–279. https://doi.org/10.1080/01973533.2014.903844

106 Burke, J., Kieffer, C., Mottola, G., & Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud? *Journal of Economic Behavior & Organization*, 198, 250–266

107 Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., ... & Volkamer, M. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. In *Proceedings of the Sixteenth Conference on Usable Privacy and Security* (pp. 259–284). Usenix. https://www.usenix.org/system/files/soups2020-reinheimer_0.pdf

108 Carstensen, L. L., & DeLiema, M. (2018). The positivity effect: A negativity bias in youth fades with age. Current opinion in behavioral sciences, 19, 7-12.

109 Langton, L., Preble, E., Brannock, D., Kennedy, E., & Pitts, W. (2024). Mass Marketing Elder Fraud Intervention: NIJ Final Report. Office of Justice Programs. https://www.ojp.gov/pdffiles1/nij/grants/308661.pdf

110 Fletcher, E., & Pessanha, R. (2016). Cracking the invulnerability illusion: Stereotypes, optimism bias, and the way forward for marketplace scam education. BBB Institute for Marketplace Trust. https://bbbfoundation.images.worldnow.com/library/daf0b5d7-c61e-4df7-abef-f1b1d8df7578.pdf

111 Wen, J., Yang, H., Zhang, Q., & Shao, J. (2022). Understanding the mechanisms underlying the effects of loneliness on vulnerability to fraud among older adults. *Journal of Elder Abuse & Neglect*, *34*(1), 1–19.

112 Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. *Symposium on Usable Privacy and Security (SOUPS)*. http://doi.org/10.1145/1572532.1572536

113 DeLiema, M., & Deevy, M. (2017). Aging and exploitation: How should the financial service industry respond (pp.153–184). In Mitchell, O.S., Hammond, P.B., & Utkus, S.P. (Eds.). *Financial Decision Making and Retirement Security in an Aging World*. Oxford University Press

114 DeLiema, M., Volker, J., & Worley, A. (2023). Consumer experiences with gift card payment scams: Causes, consequences, and implications for consumer protection. *Victims & Offenders*, 18(7), 1282–1310.

115 Federal Trade Commission (2024) "Impersonation scams: not what they used to be." Consumer Protection Data Spotlight. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/04/impersonation-scams-not-what-they-used-be

116 DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O.S.(2017).Exploring the risks and consequences of elder fraud victimization: Evidence from the Health and Retirement Study. *Michigan Retirement Research Center Research Paper*, (2017-364), 2018-06.

117 Balleisen, E. J. (2017). *Fraud: An American history from Barnum to Madoff*. Princeton University Press.

## About the author

**Marti DeLiema, PhD** is a gerontologist and Assistant Professor in the School of Social Work at the University of Minnesota. She is the Associate Director of Education for the Center for Healthy Aging and Innovation (CHAI) at the University of Minnesota, and the faculty advisor for the student-led Aging Studies Interdisciplinary Group. She also holds the 2023–2024 Fesler Lampert Chair in Aging Studies.

Dr. DeLiema believes that avoiding financial abuse and fraud is a critical component of well-being in later life, yet victimization causes millions of Americans to become financially fragile. Using both quantitative and qualitative research methods, Dr. DeLiema studies financial victimization using focus groups, in-depth interviews, surveys, and panel data. She regularly collaborates with financial institutions, AARP, the FINRA Foundation, and federal protection agencies to analyze victimization risk factors and to test efforts to inoculate consumers from fraud and abuse through enhanced consumer education and advance care planning interventions. Her research is funded by the National Institute of Justice, the National Institute on Aging, the Social Security Administration, the Administration for Community Living, AARP, and the FINRA Investor Education Foundation.

Prior to joining the School of Social Work, Dr. DeLiema was a Research Scholar at the Stanford Center on Longevity. She graduated with her doctorate from USC School of Gerontology where she conducted research on elder mistreatment in minoritized communities, evaluated outcomes of a multidisciplinary team's response to elder abuse, and analyzed the tactics scam artists use to harm older adults.

## Contributors

**Ron Barthel** is a senior leader within TIAA's Global Cybersecurity & Fraud Management organization, currently leading Cybersecurity Awareness & Client Engagement.

In this capacity Ron oversees a broad program that educates TIAA clients and the TIAA workforce on their accountability with Cybersecurity. Ron joined TIAA in 2014, previously serving as Business Information Security Officer for TIAA's institutional business and managing TIAA's cyber risk assessment function. Additionally, Ron serves as co-chair of SPARK & FS-ISAC's joint Retirement Industry Council (RIC).

Ron graduated from Fordham University with a Bachelor's degree in Computer Information Science in 1999, achieved a Master's degree in Cybersecurity from NYU's Tandon School of Engineering in 2022, and has worked in IT, IT Risk Management and Cybersecurity for over 20 years. His additional certifications include CISSP, CRISC, AWS Solutions Architect, NSA Cyber Defense, and Scrum Product Owner.

**Dale Jones,** Managing Director and Head of Enterprise Fraud Management for TIAA, is responsible for leading innovative strategies that protect client accounts against fraud threats. Dale has more than 30 years of experience fighting financial crime, including helping to build financial crime prevention teams for several Fortune 100 firms, shaping some of the best practices in the industry. While finding his love for fraud mitigation early in his career as an investigator, his experience evolved to include a suite of financial crimes leadership skills spanning fraud management and anti-money laundering disciplines.

A Certified Anti-Money Laundering Specialist and member of the International Association of Financial Crimes Investigators and the Association of Certified Fraud Examiners, Dale holds Series 7 and 24 FINRA registrations. He earned his BS in Business Administration from Saint Leo University and his graduate degree in Financial Crime and Compliance Management from Utica University.

## Contributors (continued)

**Surya Kolluri** leads the TIAA Institute and focuses his research efforts on retirement and healthy aging. The Institute, now celebrating its 25th anniversary, conducts cutting-edge research in the areas of financial and longevity literacy, lifetime income, retirement plan design and behavioral finance for higher education and the broader nonprofit sector.

Surya sits on the board of the Wharton Pension Research Council, the advisory councils of Georgetown Center for Retirement Initiatives, the Retirement Research Center of the Defined Contribution Institutional Investment Association (DCIIA) and the U.S. Alzheimer's Association (MA/NH Chapter). In 2021, Surya received The President's Volunteer Service Award via AmeriCorps for his commitment to strengthening communities.

Surya holds an MBA from The Wharton School at the University of Pennsylvania and a master's in mechanical engineering from Drexel University. He lives with his family in Brookline, Massachusetts.

**Julie Moog,** Managing Director of Global Cybersecurity and Customer Engagement, heads TIAA's Office of Cybersecurity and Customer Engagement and is Chief of Staff for the Global Cybersecurity and Fraud Management organization, responsible for overall strategy, program management, business metrics, reporting, financial analysis, enterprise cybersecurity training, awareness and cybersecurity engagement and partnership externally.

Julie has 20 years of experience in IT risk, regulatory compliance and information security within the financial services industry, including leading the IT Risk Management team and the Cybersecurity's regulatory and audit function, and establishing and leading the Business Information Security Office for TIAA.

Julie began her career at Ernst & Young in the IT Risk & Assurance group and was an information risk manager at JPMorgan , supporting emerging markets for the Americas and EMEA. Julie holds a Bachelor of Science degree in Business Information Systems from Lehigh University.

## About the TIAA Institute

The TIAA Institute helps advance the ways individuals and institutions plan for financial security and organizational effectiveness. The Institute conducts in-depth research, provides access to a network of thought leaders, and enables those it serves to anticipate trends, plan future strategies, and maximize opportunities for success.

**To learn more, visit tiaainstitute.org.**

**Join the conversation online: @TIAAInstitute**



3997034-1126

TIAA Institute

(10/24)