



Testimony of Amy Nofziger  
Director of Fraud Victim Support  
AARP Fraud Watch Network

on

Protecting Americans' Money: Combatting Scams and Frauds Against Seniors and Savers

Before the

U.S. Senate Committee on Banking, Housing, and Urban Affairs

September 12, 2024

My name is Amy Nofziger and I am the Director of Fraud Victim Support 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 Senate Committee on Banking, Housing, and Urban Affairs for holding this important hearing, “Protecting Americans’ Money: Combatting Scams and Frauds Against Seniors and Savers.” AARP has long worked to educate consumers, support fraud victims, and improve fraud detection and prevention at financial institutions, and we look forward to working with you to spread awareness and work towards policy solutions to prevent fraud and protect fraud victims.

Fraud in America is at crisis levels. The [Federal Trade Commission’s \(FTC\) latest data](#) shows there were \$10.3 billion in fraud losses in 2023 – a dramatic increase from the \$1.9 billion in losses in 2019. The Federal Bureau of Investigation’s (FBI) numbers are even more stark. In 2023, the FBI reported \$12.5 billion in losses (compared to \$3.5 billion in 2019). And because of vast under-reporting, this is likely a small percentage of actual losses. [An AARP study in 2021](#) estimated 9 in 10 Americans encountered a fraud attempt, and 1 in 7 had money stolen from them in 2020 alone.

While the issue of fraud is not unique to older adults, it often has a disproportionate financial impact on them. According to FTC data, older adults reported higher median losses than younger adults in 2023, with a median loss of \$1450 for those age 80-plus reporting a fraud loss, compared to \$460 for those in the 20-29 age group. Older adults are often targeted by criminals because they have more money – they have had a longer time to accumulate savings and are therefore appealing targets for criminals. These losses can have significant impacts on the financial security of older Americans, as they are often living on fixed incomes and can scarce afford to lose funds to criminals.

Victims come from diverse backgrounds – criminals do not discriminate when it comes to targeting potential victims. Our Helpline has made clear to us that fraud happens to everyone – it does not matter a victims’ age, their income level, where they live, or what level of education they have. Everyone is susceptible to fraud.

For many fraud victims, the financial toll is only part of the story; [research](#) shows nearly two in three victims suffer a significant health or emotional impact. This is in part caused by the stigma associated with fraud. While society treats many victims of crime with compassion, the typical response with fraud victims is to place the blame and responsibility on the victim. There is a tendency to blame fraud victims for “falling for” a scam, not being smart enough, or not paying enough attention.

The reality is that the criminals who carry out these scams have professionalized their industry – they are experts at convincing people to send them money via a plethora of different types of scams and it is not surprising at all that they are successful. It is vital we change the narrative, as the blame and stigma currently associated with fraud not only have a devastating impact on victims, but also discourage victims from reporting fraud when it happens to them. For example, it is important that when we talk about scams and fraud, we say “criminals stole their money” rather than “they lost money to a fraudster,” which places the responsibility of the crime on the victim rather than the perpetrator. AARP has done extensive research and has developed

[resources](#) to help educate people on what language is more appropriate when working with victims.

Fraud prevention has been a top priority for AARP, and we have worked to address and prevent fraud for many years. In my testimony, I would like to share some of the initiatives that AARP has worked on in this space, including the Fraud Watch Network Helpline, which I lead. In my testimony today, I will talk about AARP's fraud prevention and fraud victim services work, trends in fraud and the top types of fraud that we see, and how victims and communities are impacted by fraud.

### **AARP Fraud Watch Network, Consumer Education, and Victims Services**

Fraud awareness and prevention have long been a priority for AARP – I myself have worked in fraud prevention and fraud victim services at AARP for 23 years. While this issue has always been a priority, our fraud prevention work has grown over time as we have increasingly heard from members that fraud is a concern for them and their financial security. The AARP Fraud Watch Network was created in 2013, and our fraud prevention work through our state offices has grown and become standardized in recent years.

AARP works with victims of fraud through our Fraud Watch Network, which offers resources to arm consumers with the knowledge to spot and avoid scams. The Fraud Watch Network Helpline is available to people of any age and you do not have to be an AARP member to use the service. In 2023, the AARP Fraud Watch Network Helpline fielded over 100,000 calls from concerned Americans reporting fraud attempts or recounting their experiences of victimization, resulting in the theft of personal information and/or finances. We have 25 intake specialists and 151 volunteers in 34 states who work virtually or from one of our two field offices. Volunteers contributed 12,000 hours in 2023. Their backgrounds include former FBI agents, Secret Service agents, company CEOs, social workers, Postal inspectors, securities attorneys, CPAs, IRS agents, professors, cybersecurity experts, among many others. The Helpline can assist consumers in more than 240 different languages. The reports received by AARP's Fraud Watch Network Helpline are sent to the FTC's Consumer Sentinel database and help to provide a more complete picture of fraud trends. AARP Fraud Watch Network Helpline has contributed data to the Federal Trade Commission's Consumer Sentinel for 5 years. The Helpline has submitted over 100,000 cases to the Sentinel, representing one of the largest sets of data from the 50+ population.

AARP does extensive community outreach through the Fraud Watch Network and our 53 AARP state offices. We hold events in communities to raise awareness about different types of fraud and scams. We also partner with law enforcement, regulatory agencies, and Attorneys General to host webinars, tele-townhalls, trainings, and other fraud prevention and awareness events. We have more than 800 volunteers nationwide who deliver educational programming at the community level and work directly with victims of fraud. Each year we reach hundreds of thousands of AARP members from coast to coast with our locally driven outreach efforts.

AARP has a Fraud Resource Center and writes extensively about fraud in the *AARP Magazine* and *AARP Bulletin*. Articles and resources include recent fraud news, information about common scams, trends in fraud, and how to recognize and avoid common scams. We also have [videos](#) that break down how scams work and how to keep yourself safe from criminals. Recent articles have included, “[Danger: Investment Scams Ahead: Learn the telltale signs of investment fraud from these recent court filings](#)” and “[Six Fast-Growing Scams Coming Your Way: Criminals are using the latest technology and a whole lot of creativity to come up with fresh ways to steal from you.](#)” These publications reach millions of Americans and fraud-related articles are some of our most-read and well-received – an indication of how worried our members are about fraud.

AARP launched a weekly podcast called *The Perfect Scam* in 2019 to highlight the different types of fraud and scams that we were hearing about from our members and callers to the Fraud Watch Network. Our host introduces listeners to those who have experienced scams firsthand, as well as leading experts who pull back the curtain on how scammers operate. In December 2023, the *New York Times* [highlighted](#) the scam podcast as a top resource to “deepen your understanding of how liars and con artists operate.” Recent episodes have focused on credit card scams, rental scams, gold bar scams, pet scams, charity scams, time share scams, arrest warrant scams, military benefit scams, romance scams, and job posting scams, among many others. Most of these stories come directly from victims we have worked with on the Helpline.

The AARP Fraud Watch Network has also developed a free program to provide emotional support to fraud victims and their friends and relatives. AARP’s [Fraud Victim Support Group](#) provides individuals with an online forum to meet and interact with others who have experienced similar events. Our sessions are a safe environment to give and receive valuable feedback and support from others who are on the road to emotional healing and recovery. Group sessions are confidential and led by trained facilitators who offer fraud education and understanding to participants, as well as time for meaningful peer-to-peer sharing and support. Participants don’t have to be the primary victim to attend – family members, partners or friends of a fraud victim are welcome and encouraged to participate. Experiencing fraud can be devastating, and these types of safe spaces can be very valuable to victims in recovering from the trauma it causes.

AARP also runs a program called *BankSafe*, which trains employees at financial institutes to detect fraud and financial exploitation. [BankSafe](#) works with the financial services industry to help them stop financial exploitation before the money leaves accounts. The program encourages industry to voluntarily adopt research-proven interventions, policies, and procedures that effectively prevent exploitation. Researchers from Virginia Tech Center for Gerontology have [studied](#) the impact of training bank and credit union staff to spot and prevent financial exploitation. The research shows significant benefits to consumers and financial institutions when frontline employees take the AARP *BankSafe* training rather than other forms of training, including a 133% increase in knowledge regarding exploitation and four times greater employee confidence in recognizing, preventing, and reporting cases of financial exploitation. *BankSafe* trained employees saved consumers 16 times more money from exploitation.

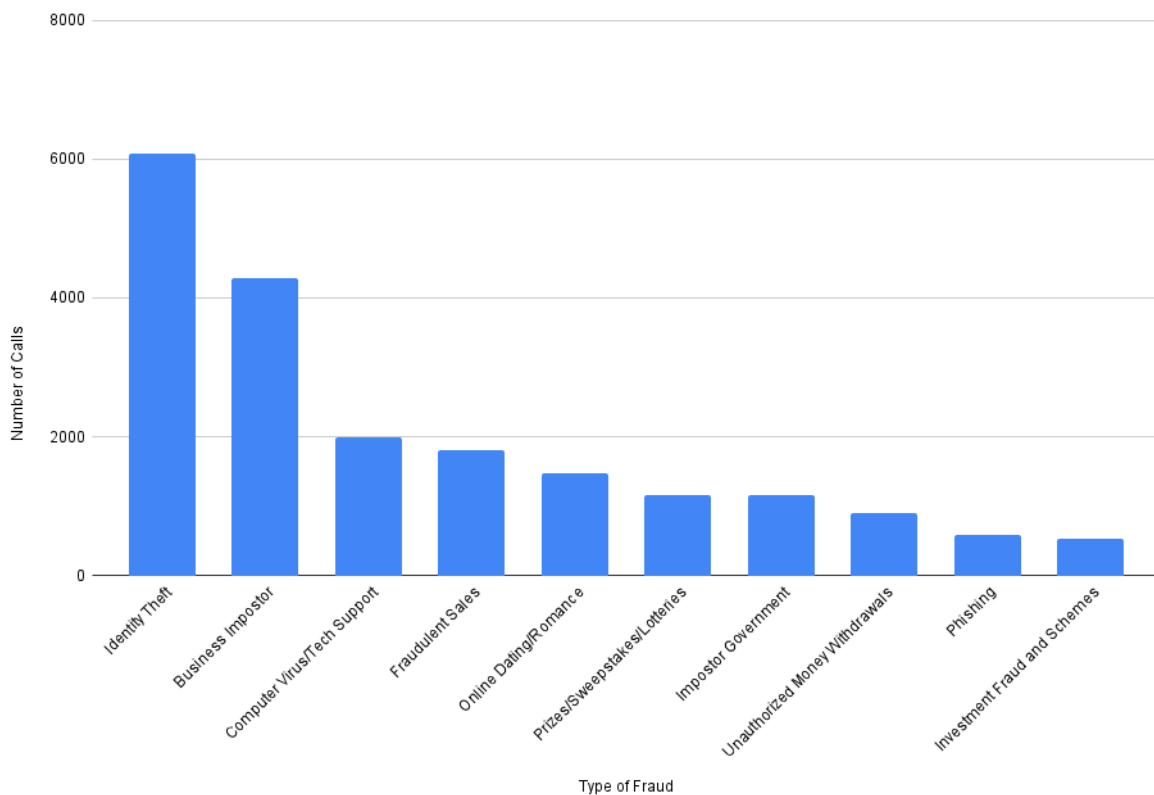
In addition to our fraud prevention awareness and victim support services, AARP conducts research on fraud to inform our work and the public at large. For example, in May 2024, we conducted research on [How Adult Consumers Feel, What They Know, and Their Actions That](#)

[Pose Risks](#). The report found that while most adults rarely or never answer phone calls, texts, or friend requests from people they don't know, a significant percentage of adults (35%) usually or always do one or more of these actions. The report also looked at how adults were maintaining security of their devices and online accounts, including the use of VPNs and two-factor authentication, downloading free apps and/or taking online quizzes on social media, and the use of different passwords on all accounts.

### **AARP Fraud Data**

In 2023, AARP received approximately 100,000 calls to their Fraud Watch Helpline. While the range of scams that people call about is vast, the top calls received in 2023 were about identity theft, business imposter scams, tech support scams, fraudulent sales, and romance scams. Below I will outline what these scams look like and share victim stories.

Top Ten Types of AARP Fraud Watch Network Helpline Calls (2023)



AARP's Fraud Watch Network Helpline also tracks the contact method used by criminals to approach their victims, as well as the payment methods requested in scams:

### Top Methods of Contact Used to Target Victims (2023)

1. Phone Call
2. Email
3. Was not contacted\*
4. Text Message
5. Internet/Online (includes social media)

\* In many ID theft cases, a victim learns about the fraud without receiving contact or when someone is checking their bank account and realizes there is a fraudulent transaction.

### Top Methods of Payment Requested (2023)

1. Gift card
2. Credit card
3. Bank account accessed
4. P2P payment app
5. Cryptocurrency

Just as the types of scams we see are varied, we see criminals use a variety of different methods to approach their victims, as well as payment methods used to steal their money. Of note, AARP has seen a large increase in the use of text messages by criminals. Older adults increasingly use text messaging, which makes them more accessible to criminals via text message. Social media is also increasing in popularity with criminals. In one example of a scam that started on social media, a woman received a Facebook message from a Brazilian singer she admired who began a long correspondence with her. The woman eventually decided to leave her husband for him. She had given him their life savings — \$300,000 — before learning he was a fraud. Phishing emails have improved in their design and content and are more likely to make it through spam filters that would have caught previous generations of scam emails. Applications with social components, such as gambling apps, word or crossword game apps, and other game apps are also increasingly used to contact potential victims.

Payment methods like gift cards remain very popular with criminals. Scammers may say they are from the Internal Revenue Service or Social Security Administration and tell a target that they owe taxes or must pay a fee to ensure their benefits continue, demanding payment in gift cards. In addition, we have seen an increase in the use of peer-to-peer platforms that are accessible and easy to use and send funds quickly. Criminals adapt to new technologies and AARP has seen a large increase in cryptocurrency as the requested payment method. We believe this is because cryptocurrency is more widely accessible, but not widely understood, and there has been a lot of “buzz” around it. It is easier to move large quantities of money quickly via cryptocurrency than other assets, including via cryptocurrency ATMs, which allow people to insert cash and then send cryptocurrency to a cryptocurrency wallet address (in the case of scams, to the wallet of a criminal). Cryptocurrency moves quickly and transactions are irreversible, which can pose challenges for recovering the funds.

A recent Helpline case using cryptocurrency involved a 69-year-old Greenfield, Ohio, woman who started a romance online with a gentleman who said he was an American architect in Cape Town, South Africa. He told her he was stuck there because his investors were late paying him

on a building project. He provided a LinkedIn profile, and a copy of his passport. She opened a bank account that he wanted her to use to convert his funds into crypto when he received them. She became suspicious that this was a scam when she tried to verify that he was in fact a licensed architect in Massachusetts as he had claimed and was not able to. Our Helpline volunteers helped her compile a complete report that she could send to law enforcement and helped her identify where to report the crime.

### ***Identity Theft***

Identity theft occurs when someone obtains someone else's personal information, such as a Social Security number, home address, date of birth or bank account data, and uses it for fraud or other illicit purposes. Identity fraud cost 40 million Americans a combined \$43 billion, according to a [AARP-sponsored report from Javelin Strategy & Research](#). While identity theft losses have decreased (2022's losses were \$9 billion less than 2021's) in large part due to the efforts of the financial services industry, this remains a significant problem and is the top type of fraud reported to the Fraud Watch Network.

Scammers' methods 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 utilities, banks or big tech firms to get their hands on identifying information, or they send phishing emails with links that can infect your device with data-harvesting malware. Scammers can also buy peoples' personal information, such as their name, address, Social Security Number, banking information, etc. online. There are many [illicit websites](#) that now sell personal information gathered in data breaches and hacks. All of this allows criminals to use social engineering to better target their victims and to be more believable.

Most often, scammers claim to represent government agencies, soliciting personal or financial data on the pretext of helping you collect benefits or navigate bureaucracy. That includes a recent surge in criminals pretending to be someone in your social network claiming they represent the Internal Revenue Service (IRS), then guiding you toward fake websites or phone numbers where you'll be asked for personal information.

Once they have your private data, scammers may use it to open credit accounts and make big-ticket purchases you might not discover until the bills come due. They might get medical treatment, file tax returns, or take out loans in your name. The costs are counted not just in money but in time spent chasing down phony accounts, repairing damaged credit and reestablishing your identity with government and financial institutions.

### ***Business Imposter Scams***

In business imposter scams, criminals impersonate well-known and/or trusted businesses, such as a victims' bank, retailer, a utility company, mortgage provider, charity, or lawyer or debt collector. For example, criminals may pretend to be your financial institution and call victims telling them that their account has been compromised. However they present themselves, the message will be urgent: a bill is overdue; an account has been compromised; a cause needs your support; a loved one is in trouble. Resolving the problem is a simple matter of making an

immediate payment (such as by gift card or wire transfer) or providing personal data such as a Social Security number, bank account number, or login information. Many impostor scams are quick hits — the goal is to cajole or frighten you into making a rash decision, then disappear after stealing money from you for a reason that sounds plausible and by a method that may not be traceable.

#### Business Imposter Scam Example:

Magis, who reached out to AARP’s Fraud Watch Network, experienced a complex bank impersonation scam and 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. She faces a substantial loss of Social Security retirement benefits due to the withdrawals from her retirement accounts, which put her income in the highest withholding category. Magis has suffered significant stress and faces the possibility of being forced to sell her home and face homelessness.

#### ***Tech Support Scams***

This is one of the most common scams in the United States. According to Microsoft, in 2015 an estimated 3.3 million people — many of them seniors — were victimized by a [tech-support con](#), at a total cost of \$1.5 billion. That's one American who has an average of \$454 stolen from them nearly every 10 seconds. Here's how tech support scams typically unfold: You get an unsolicited call from someone claiming to be with Microsoft or Windows tech support, who says viruses have been detected on your computer. In order to protect your data, you are told to immediately call up a certain website and follow its instructions. A dummy screen may appear that shows viruses being detected and eliminated, but in reality malware is being installed that allows the scammer to steal your usernames and passwords, hold your data for ransom or even use the webcam to spy on you.

AARP has continued to see these scams with the criminals becoming more aggressive, posing as anti-virus software representatives, sending fake invoices, and increasingly focusing on accessing victims’ bank accounts once they have remote access to their computer, as well as attempting to take over the victims’ phones (in order to receive two-factor authentication text messages) and other devices.

#### Tech Support Scam Example:

A woman from Southern California who reached out to AARP’s Fraud Watch Helpline, Helen, a retiree in her 80s, was reading her sister’s obituary on the web when a pop-up screen suddenly appeared, announcing that her computer had been infected with a virus. “Do not turn off your computer!” a loud voice warned through the computer’s speaker. Helen was instructed to call the phone number that appeared on her screen, according to her son, a retired U.S. intelligence agency official who — with her permission — shared her story with AARP. She soon found herself talking to someone who claimed to be a tech support staffer from Microsoft. He asked for



her cellphone number, and he was likely able to use that number to look up where she banked because such information exists in dark web databases. The fake tech support staffer told her, “There are 36 hackers in your computer right now.” She trusted him because, after all, he knew where she banked, and she hadn’t divulged that information, or even her name. Then he 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, possibly triggered by a malicious ad planted on a website. 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. She lost most of her retirement nest egg to the criminals before a bank fraud investigator intervened, convincing her to speak to her family about what she was doing.

### *Fraudulent Sales*

Fraudulent sales scams is a wide-ranging category that includes a number of different types of sales scams. For example, a victim may find a website to purchase an item they think is legitimate, but it is a fake website and the money they thought they were spending is actually stolen from them. There are also websites that sell fake goods, such as fake medication. Sites like Craigslist or Facebook Marketplace also have been leveraged by criminals to steal money. For example, scammers may ask for payment in advance and then never deliver goods, or criminals may ask victims to send them “test payments” via peer-to-peer apps to confirm their accounts work before making off with the money.

In 2019, federal officials warned of possible fraud when buying online at popular sites such as Craigslist and eBay after an international organized crime group was [charged](#) with cheating thousands of Americans out of millions of dollars. Members of a Romanian-based crime group were arrested for pretending to sell cars and other high-ticket items online — only the items never existed. In some cases, the scammers impersonated members of the U.S. military and said they needed to sell the advertised item because they were deploying overseas, according to a federal indictment. The defendants “allegedly orchestrated a highly organized and sophisticated scheme to steal money from unsuspecting victims in America,” says Assistant Attorney General Brian Benczkowski. One defendant posed as Air Force Sgt. Judith Lane, who used a phony profile on social media and a fake Gmail address and advertised cars for sale on Facebook, authorities said. Lane wasn’t in the Air Force, wasn’t a sergeant and wasn’t even a woman, authorities said. Hiding behind the fake persona was a 28-year-old man named Ionut Ciobanu who, like most of the defendants, is a Romanian.

AARP has also seen pet scams become popular – criminals impersonate breeders, creating slick websites full of filched puppy pics that offer popular breeds at steep discounts. Or they post ads on social media or online marketplaces like Craigslist, posing as pet owners forced by personal or financial circumstances to put a beloved kitty or pooch up for “free” adoption to a loving family willing to cover shipping costs. If you respond, they’ll ask due-diligence-type questions about your home situation and experience with pets, but the only query they really care about is whether you’ll wire a payment. They’ll direct you to a website for a transport company (also

bogus) so you can track your nonexistent pet's progress, which will invariably be delayed by contrivances requiring more money, such as insurance or a special travel container. One scam ring [busted by federal authorities](#) in 2020 told would-be puppy buyers that shipments were held up by canine exposure to COVID-19. In these scams, criminals are betting that victims' emotional investment in the anticipated pet will keep the payments coming, into the hundreds or even thousands of dollars. If the victim becomes suspicious, they may resort to threats, claiming the animal will die or they will be charged with animal abandonment.

### ***Romance Scams***

Romance scams are on the rise. According to the FTC, people reported a record \$547 million in losses to romance scams in 2021 – up about 80% from the FTC's 2020 reports. Adults of all ages are going online in hopes of finding love and companionship. Unfortunately, cyberspace is full of criminals eager to take advantage of people looking to find love, and their ranks are growing.

The con typically works something like this: The victim posts a dating profile and up pops a promising match — good-looking, smart, funny and personable. Supposed suitors might also reach out on social media; many people who lost money to a romance scam reported that it started on Facebook or Instagram, [according](#) to the FTC. The criminal will use pictures of an attractive person. (You can check out Social Catfish's list of the top 100 photos used for catfishing (using a fake identity to lure someone into a romantic relationship)). A potential mate may claim to live in another part of the country or to be abroad for business or a military deployment. But he or she seems smitten and eager to get to know you better, and suggests they move your relationship to a private channel like email or a chat app.

Over weeks or months, the victim grows closer to the scammer. They may make plans to meet in person, but for their new love something always comes up. Then they get an urgent request – there's an emergency (a medical problem, a visa issue, a business crisis) and the victim's online companion needs them to send money fast, usually via gift cards, prepaid debit cards, cryptocurrency, or a bank or wire transfer. They'll promise to pay it back, but that will never happen. Instead, they will keep asking for more until the victim realizes it's a scam and cuts them off. These sorts of scams are particularly emotionally impactful for victims because not only have they had money stolen from them – they are now going through a breakup from someone they loved and trusted. While romance scams are not new, AARP has seen increased emotional impact from the fallout of these relationships since the beginning of the COVID-19 epidemic. There has also been an increase in extortion attempts, in which a scammer tells their victim that if they do not pay, they will share explicit videos or photos with the victims' friends, family, church, school, etc. Finally, we have seen increased losses in these types of scams in recent years.

### **Romance Scam Example:**

Kate, a suburban Philadelphia widow did not plan to date again until a handsome “surgeon” asked to be her Facebook friend. Soon “Tony” became romantic and professed his love. Though the two never met in person, Tony talked about marriage, said he purchased a ring and asked her to look for a house for them near where she lived. All the while, he kept prodding her for gift

cards — and promising he'd repay her. He even provided her with a password for a purported bank account with a \$2 million balance. The two were to meet for the first time in December 2020; he said he'd fly to Philadelphia International Airport. She had her hair and nails done and waited at home in her best dress for his call. A bottle of wine was chilling. Hours passed, without a word from him. A day later, Kate got a call from a man who claimed to be a lawyer saying Tony had been arrested at the airport because someone planted drugs in his luggage. Tony was said to be confined to a Philadelphia jail and needed \$20,000 for bail— money she did not have. Later, Tony called and messaged to urge her to get the money somehow, even if it meant lying to her family. She refused. But her reservations melted away when he complained about the “awful” food in jail and asked for small sums, which she sent. Then Tony's story got even more improbable. He called saying he was in Jordan; he said he'd been released so he could raise the bail money. She said that wasn't the way it worked: You don't get out of custody to raise bail. Finally, she saw the romance for what it was — phonier than a \$3 bill. Though Tony was fake, her heartbreak was real. What hurt most, she said, was “losing his love and losing the family I thought I was going to have and what my new future was going to be... That is much harder to deal with than losing the money.” She ended up losing everything she owned — including her home — in the coldhearted scam that played on her emotional vulnerability and kindness.

### **The Impact of Fraud**

Through our initiatives with the Fraud Watch Network, AARP frequently hears directly from victims about the profound effects fraud has had on their lives. These individuals recount how scams have caused financial devastation and emotional turmoil, highlighting the severe consequences of such crimes. Family members share the ripple effects on their households. Our work also reveals the emotional toll on first responders and victim service providers who assist these victims. Fraud significantly impacts our communities, and it is crucial to understand its various effects.

This financial loss can result in greater reliance on credit cards, which can lead to debt and impact the victim's credit score, making it more difficult for them to obtain loans, mortgages, or rent an apartment. Victims may lose their home and be forced to move in with family members or friends. They may become reliant on social safety nets, and this can strain community resources. Victims have reported that where their retirement accounts have been drained by criminals, this has affected their Social Security benefits, as retirement account withdrawals can result in higher income brackets and greater taxes on both their lost retirement funds and their benefits.

There are also serious emotional ramifications of fraud. Victims report feeling frustration, anger, mistrust, and sadness after experiencing fraud – and some unfortunately commit suicide. According to a FINRA [study](#), two-thirds of fraud victims reported experiencing at least one non-financial cost of fraud to a serious degree. These included severe stress (50%), anxiety (44%), difficulty sleeping (38%), and depression (35%). Victims who lose more money are more likely to incur more non-financial costs. These emotional impacts of fraud often lead victims to not report that crimes have been committed against them because of the guilt and shame they may feel. This contributes to significant underreporting to law enforcement, resulting in an unclear picture of the true scope of the problem and where to focus investigative efforts.

Many victims feel ashamed to even report the fraud that has happened to them – and often they blame themselves rather than the criminals who have stolen their money. A contributing factor is the stigma, shame, and blame associated with being a victim of fraud. Victims report hearing “How could you fall for that?” or “I can’t believe you were duped!” when they tell others what has happened to them. The language law enforcement, industry, and victim services providers use and the way that they treat fraud victims [matter](#) greatly. Rather than scolding or shaming victims, we must treat them with empathy and [without judgement](#) – “This is not your fault.” or “Scammers are master manipulators, and you are a victim of crime.” AARP has done research on this issue, and published [resources](#) to help people use the right language when speaking to and about victims.

**HERE ARE EXAMPLES OF WHAT TO SAY:**

**INSTEAD OF THIS:**

**How could you fall for that?**

**SAY THIS:**

**This isn't your fault – you experienced a crime.**

**INSTEAD OF THIS:**

**How much money did you give them?**

**SAY THIS:**

**How much did the criminal steal?**

The story of one victim who reached out to the Helpline, Mo, does a good job of highlighting the emotional impact of fraud. Mo was the victim of a devastating investment scam that resulted from meeting someone online who eventually convinced him to invest in cryptocurrency. The criminals involved stole millions from Mo and his family. He continues to beat himself up for the damage this has caused to his marriage and his two children. He has suicidal thoughts, but also realizes he needs to be around for his family. He constantly asks himself, “how could I be so dumb and stupid?” This is unfortunately a very common experience for fraud victims.

In another story, a Los Angeles woman talks about the impact of being targeted by a criminal impersonating a TV journalist she admired. She had sent him a message telling him she liked his work when she found his social media profile online. In the end, the criminal impersonator stole \$70,000 from her via wire transfer, gift cards, and Bitcoin. She was left with \$500 to buy groceries and pay her bills. She said, “I’m crying every day. I don’t know what to do. And I’m taking money out of my retirement and my savings that I had saved for years.” At one point her thoughts turned suicidal. She drove herself to a hospital, where she was quickly admitted. When she told the psychiatrist on duty her story, he said, with sympathy, “You’ve been scammed.” She’s been dealing with the emotional fallout ever since.

Fraud support services are an important component in helping victims process and recover from fraud. AARP's Fraud Watch Network serves a very important role for victims, as one of the few resources with people willing to listen and help victims process what has happened to them, as well as help them report the crime. Many of the victims share with our Helpline volunteers that they have no one in their lives who will understand what is happening and they are embarrassed to talk to them about it. We cannot allow victims' horrible experiences to leave them alone and isolated. More than anything, they need support – and until families and friends understand this, AARP and other victim support groups will be there to help them recover. Not only do we need to focus on victim support, but we must support families too. We hear from many families that even when they are supportive and compassionate to their loved ones, they themselves have significant guilt or confusion on why this happened. We hear from grandchildren whose grandparents have been a victim of a grandparent scam have survivors' guilt and need support. Understanding the emotional impact of fraud is critical to changing how we respond to victims.

### **Conclusion**

I would like to emphasize the profound and multifaceted impact of fraud I witness daily through my work at AARP. I see firsthand the emotional and financial devastation that fraud wreaks on individuals, especially older adults, and our communities at large. In recent years, we have observed a troubling increase in both the prevalence of fraud and the losses associated with fraud. To stop fraud, we will all have to work together.

In our ongoing work with the Fraud Watch Network, AARP directly encounters the profound emotional and financial impacts of fraud on individuals and families. Victims often describe severe financial losses. In addition, the emotional toll of fraud is devastating; victims frequently report intense feelings of frustration, anger, sadness, and even suicidal thoughts. This is exacerbated by the stigma and self-blame many victims face.

We must encourage a culture of reporting and ensure that victims receive the consistent compassion and support they need, regardless of where they live or to whom they report fraud. This will not only aid in their recovery, but also provide law enforcement with critical data to understand and combat fraud effectively.

Addressing fraud requires more than piecemeal solutions; it demands a holistic and coordinated approach. We need a collaborative effort that brings together victim services providers, industry stakeholders, and government agencies. Each of these groups plays a crucial role: victim services offer essential support and advocacy, industry players are on the front lines of detection and prevention, and regulatory and law enforcement agencies can bring justice for victims and aid in victim restitution.

We thank this Committee for bringing attention to this important issue and look forward to working with you to combat fraud and find comprehensive solutions to prevent it.