Statement of Steve Weisman J.D.

Senior Lecturer, Bentley University

Editor of Scamicide.com

Of Counsel: Margolis, Bloom & D'Agostino

United States Senate

Special Committee on Aging

November 16, 2023

Chairman Casey, Ranking Member Braun, and members of the Senate Special Committee on Aging:

My name is Steve Weisman, I am a lawyer with the firm of Margolis, Bloom & D'Agostino, a Professor at Bentley University where I teach White Collar Crime, author and the editor of Scamicide.com, where each day I provide new information about the latest scams, identity theft and cybersecurity. Scamicide was named by the NY Times as one of the three best sources for information about Covid related scams.

When it comes to frauds and scams targeting seniors, I am here to tell you that things aren't as bad as you think – unfortunately, they are far worse. According to the FTC's Consumer Sentinel report for 2022, older Americans reported more than $1.6 billion in losses to frauds and scams. This number is undoubtedly lower than the actual figure because many seniors, for a variety of reasons, including embarrassment or shame, fail to report the scams perpetrated against them. FTC estimates that in 2022 the actual amount lost by seniors to scams could be as high as $48.4 billion.[1]

And now with Artificial Intelligence, the scams are getting worse. AI has become a sophisticated weapon that can be deployed by even the most unsophisticated scammers.

In 2022, older Americans had higher reported losses to scams than younger people and those ages 80 and older reported the highest individual median losses among all age groups.[2] Why are seniors so much more likely to be targeted for scams? To some extent it may reflect the thinking exemplified by the infamous bank robber, Willie Sutton, who when asked why he robbed banks responded, "Because that is where the money is." Many seniors may have a lifetime of accumulated savings that make them a tempting target for scammers. It has also been thought that seniors might be more susceptible to scams due to being more trusting, and two studies may have found a physiological basis for that opinion. A 2017 study conducted by researchers at Cornell University and published in the Journals of Gerontology concluded that naturally occurring changes in the brains of older people make them vulnerable to

[1] Protecting Older Consumers 2022-2023, A Report of the Federal Trade Commission, October 18, 2023

[2] Protecting Older Consumers 2022-2023 A Report of the Federal Trade Commission October 18, 2023

financial exploitation. The changes noted were in a part of the brain that signals risk, as well as another part of the brain that controls the ability to read social cues.[3]

A similar study conducted in 2012 by researchers at the University of Iowa found that naturally occurring changes in the prefrontal cortex of the brain make older adults less skeptical and therefore more likely to be victimized by a scam.[4]

These changes in the brain can and are exploited by scam artists, the only criminals we refer to as artists, who often appear to have a knowledge of psychology that Freud would have envied.

So, who is perpetrating these scams?

Scammers are cybercriminals who can be located anywhere in the world or just around the corner. They can be both sophisticated hackers and unsophisticated criminals using data, technology, malware, and delivery systems they lease on the Dark Web. They can also be the criminals whose business model is to create the malware and perpetrate massive data breaches, and then lease these tools to less knowledgeable criminals.

They are gangs in Jamaica. They are call centers in India. And unfortunately, they are also family members and caregivers.

I will utilize my testimony today to discuss the common scams targeting older adults, where and how older adults are vulnerable, how Artificial Intelligence is being used to support scammers—and fight back—and how we can better protect older adults from scams.

COMMON SCAMS TARGETING OLDER ADULTS

Investment Scams

For seniors, investment scams result in the largest losses, with losses increasing 175% last year from the previous year.[5] Too often people fail to do the necessary due diligence when investing, for fear of missing out on the next big trend. They invest in things they do not understand with people they have not vetted. Bernie Madoff, of all people, actually blamed his victims for their losses saying that anyone who actually looked at what he did would have known that what he promised was impossible.

"Too good to be true" guaranteed returns that should raise red flags are ignored by many, particularly when they involve affinity fraud. Affinity fraud occurs when a scammer purports to share a connection with the target, whether it be a religious, racial, ethnic, or other connection, in order to build trust. My motto is, "Trust me - you can't trust anyone."

[3] The Journals of Gerontology: Series A, Volume 72, Issue 10, 1 October 2017, Pages 1365–1368, https://doi.org/10.1093/gerona/glx051
[4] https://www.frontiersin.org/articles/10.3389/fnins.2012.00100/full#h4
[5] Protecting Older Consumers 2022-2023, A Report of the Federal Trade Commission, October 18, 2023

And of course, when it comes to investment scams, cryptocurrency scams lead the way; many people with no knowledge of cryptocurrency rush to invest and fall prey to scammers. According to the FBI's Elder Fraud Report, in 2022, reported losses due to investment fraud for older adults increased by 300 percent from 2021.[6] The FBI attributes this to the increase in cryptocurrency-related investment scams.

Lottery Scams

While investment scams resulted in the greatest losses to Americans over 60 years of age, Americans ages 80 and over lose the most money to lottery scams.[7] It is hard to win a lottery. I can personally attest to that, but is it impossible to win a lottery that you have not entered. However, scammers such as those operating the infamous Jamaica lottery scam, in which a scammer calls from a foreign country and tells the victim they have won a prize in a foreign country, continue to convince seniors that they have won the lottery. However, in order to claim their prize, they need to pay income taxes or administrative fees first. Victims of these scams continue to pay the scammers. Discovering you have been victimized by scammers, using this scheme or any other, can be devastating: there have been reports of suicide among victims of a lottery scam.

Imposter Scams

Imposter scams, where scammers pose as company representatives or governmental agencies, have long been lucrative for scammers. While there are many variations of this scam, the most common variations involve scammers calling their intended victims on the telephone and posing as an employee of the IRS, the FBI or, often when targeting seniors, the Social Security Administration. Scammers also frequently impersonate delivery services like Amazon, the U.S. Postal Service, or UPS. The scammer then, under a wide variety of pretenses, demands an immediate payment via gift card, credit card, Peer-to-Peer (P2P) payment app, or wired funds. Being asked to pay any amount of money, especially through a gift card or P2P payment app, is a clear indication that the call is a scam. Alternatively, the scammer may demand the victim supply the phony governmental agent with personal information, such as their Social Security Number or Medicare Beneficiary Identifier, possibly exposing them to identity theft.

Last summer, a woman in Nashville, Tennessee, received a call purportedly from a border patrol office in El Paso, Texas.[8] The supposed border patrol agent told her that they had seized a package containing illegal drugs that appeared to have been sent by her. She was then told that someone was using her name for illegal purposes. The caller advised her that in order to protect her money, she should withdraw all of the money in her bank account and deposit it into a Bitcoin ATM account provided by the phony federal officer. She was then told that she would be getting a call from a DEA officer to arrange for her to pick up a check for the money the next day. The call, of course, never came and the money she deposited into the Bitcoin ATM was lost forever.

---

[6] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf
[7] Protecting Older Consumers 2022-2023, A Report of the Federal Trade Commission, October 18, 2023
[8] https://scamicide.com/2023/06/17/scam-of-the-day-june-18-2023-elaborate-impostor-scam-victimizes-nashville-woman/

Unfortunately, these scams can appear to be legitimate because your Caller ID may indicate that the call is from the FBI, IRS, SSA, or some other legitimate government agency or a company with which you do business. However, through a simple technique called "spoofing," a scammer can manipulate your Caller ID to make his call appear to come from whatever number he chooses.

The truth is that neither the IRS, Social Security Administration, nor any federal agency will initiate communication with you by a phone call and they will never threaten you with arrest for non-payment of a claim. No government agency will accept gift cards or cryptocurrency payments.

Romance Scams

Romance scams also pose a great risk to seniors, particularly older widows or widowers. Reports of romance scams of the elderly increased last year by 13% and losses have now exceeded record levels, with losses totaling $240 million.[9]

Romance scams generally follow a familiar pattern: scammers establish relationships online on dating websites and social media using fake names, locations, and images.

The scammer may quickly profess his or her love, and then, under a wide variety of pretenses, ask for money. Recently, some scammers have taken a different approach by opting to build trust and love over a long period of time and then offer a terrific opportunity to invest in cryptocurrency. Unfortunately, in this instance the word "terrific" is the adverbial form of the word "terrifying," and the romance scam victim loses the money invested through the scammer. The scammers in romance scams often pose as Americans working abroad or in the military serving overseas. Recently, a ruse used by romance scammers involves the scammer posing as a United Nations doctor working in Syria.

There are various red flags to help you identify romance scams—sadly, the most important thing to remember is to always be skeptical of anyone who falls in love with you quickly online without ever meeting you in-person, and anyone who, early into the relationship, asks you to send them money to assist them in an emergency. Be skeptical.

Grandparent, or Family Emergency, Scam

By now, many people are somewhat familiar with the grandparent or family emergency scam, within which a family member receives a telephone call from someone posing as their loved one who has gotten into some trouble, most commonly a traffic accident, legal trouble, or medical problem, in a faraway place. In grandparent scams, the scammer pleads for the grandparent to send money immediately to help resolve the problem and begs the grandparent not to tell mom and dad. This scam has been perpetuated for approximately fourteen years, but it is getting worse. We have AI to thank for that.

[9] Protecting Older Consumers 2022-2023, A Report of the Federal Trade Commission, October 18, 2023

It is a sad commentary on life today that every grandparent, or really any family member, should create a safe word with their loved ones to be used to identify themselves in a real emergency.

Tech Support Scams

Tech support scams increased by 117% last year for seniors; older adults are over six times more likely to report losing money to this scam than younger adults.[10] Victims of this scam are tricked into believing there is a problem with their computer that requires the expensive services of scammers.

The most common tech support scam starts with a popup on your computer that identifies security problems. The popup contains a telephone number for you to call to fix the problem. If you call the scammer in response to concerns about your computer, they often ask you to enable remote access to your computer in order for them to assess the problem. Providing remote access to anyone can lead to a myriad of problems, including identity theft and the downloading of ransomware. The truth is Apple, Microsoft, Dell, or any other tech company will never ask for remote access to your computer to fix a problem.

Whenever you get a pop-up, email, or text message that appears to tell you that you have a security problem with your computer, you should never click on any links in the message nor call the telephone number provided. If you are concerned that you may be experiencing a real security problem, you can contact tech support, or your device manufacturer, directly by phone or by email using the phone numbers and email addresses you can find on their respective websites.

WHERE ARE THE ELDERLY VULNERABLE?

Phone

While older Americans reported being scammed online through online shopping scams, phony websites, apps, and social media twice as much as they reported being scammed on the phone, the average losses suffered by seniors victimized by phone call scams were more than twice as much as online scams. Scams originating through text messages also resulted in higher losses than scams originating online.[11]

In 2022, imposter scams were the most common phone call scams, followed by lottery scams.[12] Bank imposter scams frequently start via text message, with the scammer telling the targeted victim that his bank account is frozen and that they need to provide their username and password to the scammer to unfreeze the account.

Scammers can make a large number of calls or text messages using computers rather than actual phones. Scammers also use prerecorded robocalls to contact their victims. Illegal robocalls can easily be made by computers using Voice over Internet Protocol (VoIP) accounts, which are a way to make voice calls using a broadband Internet connection instead of a regular phone line. Unfortunately, even if

[10] Protecting Older Consumers 2022-2023, A Report of the Federal Trade Commission, October 18, 2023
[11] Protecting Older Consumers 2022-2023, A Report of the Federal Trade Commission, October 18, 2023
[12] Protecting Older Consumers 2022-2023, A Report of the Federal Trade Commission, October 18, 2023

your Caller ID indicates the call is legitimate, spoofing, like in imposter scams, may have enabled the scammer to imitate an official phone number.

In an effort to stop VoIP calls from overseas, FTC took action against VoIP service providers here in the United States. They identified 24 service providers used to bring illegal robocalls into the United States and demanded they stop their services from being used for illegal activity. All but two complied with the demand.[13] Last summer, the Federal Communications Commission (FCC) imposed a record fine of nearly $300 million on an international network of companies, including Virtual Telecom, for violating a variety of federal laws. These companies were responsible for more than five billion robocalls to more than 500 million people in a mere three-month period in 2021.[14]

The good news is that actions by the federal government and the telecom industry to reduce robocalls have worked; Americans reported receiving 21% fewer robocalls in the first half of 2023 compared to the first half of 2022; however, the amount of money lost to robocalls went up from $30 billion during the first six months of 2022 to $33 billion for the first six months of 2023, indicating that much work still needs to be done.[15]

Email

Phishing emails, and the more specifically targeted spear phishing emails, use social engineering to lure the targeted victim to click on a link, download an attachment, make a payment, or provide personal information. Phishing emails are often a starting point for scammers, enabling them to access victims' computers, install malware, and even perpetuate data breaches. Phishing emails are sent out in huge numbers with nothing in the email that truly relates to the intended victim. Often, they may appear laughably outrageous, weeding out anyone who shows skepticism. Spear phishing emails, however, are a different story: they come with your name in the salutation and they have information about their targeted victim that makes them more believable and therefore more dangerous.

In 2021, Google released a study in conjunction with researchers at Stanford University, in which they studied more than a billion malicious emails targeting Gmail users. The study found the number of phishing and spear phishing emails users received totaled more than a hundred million each day.[16]

The most common phishing emails appear to come from social media websites, such as Instagram and Facebook, online services, such as Netflix and Amazon, banks, or email carriers, like Gmail or Yahoo. Being aware of this and being skeptical of emails that come from these parties is the first step in safeguarding yourself against phishing emails. In most instances, spear phishing emails are constructed to convince you that there is some emergency that requires your immediate attention.

---

[13] https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-ramps-fight-close-door-illegal-robocalls-originating-overseas-scammers-imposters

[14] https://www.fcc.gov/document/fcc-assesses-nearly-300m-forfeiture-unlawful-robocalls

[15] https://www.robokiller.com/blog/2023-mid-year-report-takeaways

[16] https://storage.googleapis.com/pub-tools-public-publication-data/pdf/869f2c1e6b77a86525e1ac65d3274aa62c0bd0ae.pdf

Internet of Things

The Internet of Things is made up of a broad range of devices connected to the Internet including home thermostats, security systems, medical devices, refrigerators, smart televisions, cars, and even children's toys. In recent years our homes have become filled with these devices, including the AI-powered Alexa and Siri.

In 2018, the FBI began to warn consumers about the dangers posed by the hacking of various devices that make up the Internet of Things. Cybercriminals can hack into devices that are a part of the Internet of Things to enlist these devices as part of a botnet by which they can distribute malware. They can also hack into Internet of Things devices to access your home computers to steal information for purposes of identity theft or theft of personal data, including passwords.

The risks are extreme, but there are some basic steps you can take to protect yourself. Most of the devices that make up the Internet of Things come with preset passwords that are easily discoverable by hackers. Change the preset password and make sure you have a unique password for each of your Internet of Things devices, and use dual factor authentication whenever you can for all of these devices. It is also important to set up a guest network on your router exclusively for your Internet of Things devices. This is important so that you can keep the sensitive information you have on your computer or laptop from being accessible through the hacking of any of your Internet of Thing devices. Configure network firewalls to block traffic from unauthorized IP addresses and disable port forwarding to limit access of your router from outside sources. Make sure you install the latest security patches as soon as they are available.

Make sure your router is secure and use its whitelisting capabilities which will prevent your device from connecting to malicious networks. Routers are a critical part of your smart home security. Check to see if it will automatically download and install the latest security updates from the manufacturer. If your router is an older router that does not have this capability, you should check the manufacturer's website regularly for the latest updates. However, you are probably better served by getting a newer, more secure router.

Social Media

Social media has also proven to be fertile ground for scammers targeting older Americans. According to the FTC, the losses by older adults to scams that started on social media went up from $163 million in 2021 to $277 million in 2022.[17]

Social media scams take many forms, but are most often based on us trusting the people we encounter as friends on social media. Scammers harvest information their victims post on their social media accounts to learn about who they are and what their interests are and use that information to target their victims with a wide variety of scams including investment scams and romance scams.

[17] Protecting Older Consumers 2022-2023, A Report of the Federal Trade Commission, October 18, 2023

It's nice to have friends, but people shouldn't accept friend requests from everyone who asks to be their friend on social media. Further, communications on social media are not trustworthy merely because they appear to come from your friends. Often social media accounts are hacked or cloned and the scammers, posing as your friend, leverage the trust that you have in your friends to lure you into phony investments, phony products, and romance scams.

Years ago, there was a cartoon called Pogo who is famously quoted as saying, "We have met the enemy and he is us." That sentiment could describe the relationship many people have with social media. They share details of their lives online without recognizing the opportunities they are creating for scammers.

Security questions are a perfect example of this. When you forget your password, all you need to do to solve the problem is answer a simple security question you have chosen. Common security questions include your mother's maiden name, the name of your first pet, or your first car. Unfortunately, this type of information can often be found by a scammer on social media, thus enabling them to gain access to your online bank account, or any other account where you may have used such a security question.

Users should enable dual factor authentication to ensure that even if your password is compromised, your account is protected. Additionally, for security questions, you can merely provide a nonsensical answer. If the question is your mother's maiden name, you can use an answer such as "grapefruit" because there is no rule that says you need to answer the security question literally. Using a nonsensical answer such as "grapefruit" guarantees no one is going to be able to identify the answer, and it is so ridiculous that you will certainly remember it.

ARTIFICIAL INTELLIGENCE

<u>AI and Phone Scams</u>

AI has created additional opportunities for phone call scams; AI can be used to remove foreign accents from scammers' voices, making them perhaps appear more reliable to the target. AI can also be used by phone scammers to create robocall scripts that can enable conversations with their targeted victims. Additionally, as discussed earlier, AI voice cloning technology can be used by scammers to make their targets believe they are speaking with their loved ones, or other familiar figures.

Fortunately, while AI is a tool that can be misused by scammers, it is also a tool that can be used by the good guys. Machine learning algorithms can learn to recognize patterns in robocalls. Once these patterns have been identified, the algorithms can block calls that match these patterns. In addition, by using AI natural language processing (NLP) technology, the content of robocalls can be analyzed and, if determined to be a robocall, service providers can block the call. AI also can be used to combat spoofing by analyzing the caller's true phone number and block the call if spoofing is identified. Finally, AI can be used to transcribe a call, making it easier to recognize scam calls and track patterns.

<u>Phishing Emails and AI</u>

As bad as a threat as socially engineered spear phishing emails have presented in the past, they are far worse now because of AI. Through the use of AI, scammers can create more sophisticated and effective

spear phishing emails that are more likely to convince a targeted victim to either provide personal information that can lead to identity theft, click on a link and download dangerous malware, or fall for a scam. Phishing emails that have originated overseas in countries where English is not the primary language often, in the past, could be recognized by their lack of proper grammar, syntax, or spelling; however, AI has solved those problems for foreign scammers, and their phishing emails will now be more difficult to recognize.

Fortunately, AI can also be an effective tool in combatting AI enhanced spear phishing emails. Machine learning algorithms can analyze vast amounts of data to identify patterns and trends associated with spear phishing emails. These algorithms can not only be used to recognize indications of spear phishing, but can also continually learn, adapt, and predict new forms of spear phishing emails.

Social Media and AI

Scammers have always mined social media for personal information that they can leverage to scam their victims and also as a trusted delivery system for scams. AI has only made it worse. Scammers use AI to set up social media bots, automated software applications programmed to appear to be real people on social media. In the past, the lack of sophistication in some bots made them easy to identify, but now AI has enabled scammers to create large numbers of believable bots used to promote numerous scams, particularly involving cryptocurrency. In addition, in the past, the gathering of personal information through social media was a time consuming effort for scammers, but now through AI vast amounts of information can be gathered to be used to craft effective scams.

AI's Use in Scams

With just about every form of scam, scammers are using AI to make them more effective.

In romance scams, the scammers can use AI to create fake profiles on multiple dating platforms and utilize AI to write a grammatically correct biography, making the scam easier for scammers in foreign countries where English is not the primary language. They also may use AI to create photographs, or deepfakes.

In family emergency scams, through the use of readily available AI voice cloning technology, a scammer, using a recording of the grandchild's voice obtained from a voicemail message, YouTube, TikTok, Instagram, or anywhere else the grandchild might post a video with audio, can create a voice clone and place a call to the grandparent. The audio will sound exactly like that of the grandchild, and all it takes is AI voice generating software and as little as 30 seconds worth of the grandchild's voice.[18]

AI's application is not limited to these examples—and AI's use by scammers will likely proliferate without widespread public education and regulation.

[18] https://medium.com/@todasco/deep-fakes-for-all-the-proliferation-of-ai-voice-cloning-ecee0a461dac

PROTECTING SENIORS

So how do we protect seniors from scams?

Forewarned is forearmed. Alerting the public as to telltale signs of scams and how to recognize them is a key element in protecting seniors. I do this each day through Scamicide.com and this committee also does this through publications such as its Fraud Book publication which contained much useful information.

The criminal laws that we already have are sufficient to criminalize these scams. I believe the focus should be on preventing the scams and the best way to do this is through education. The *Stop Senior Scams Act* championed by Senator Casey is a great step in the right direction, particularly as it applies to steps to be taken to reduce the use of gift cards and wire transfers, which are preferred methods of payments to scammers.

Regulation of AI is a critical element to protect people from AI-enhanced scams; the President's recent Executive Order will help. In addition, FTC has regulatory authority over AI through Section 5 of the FTC Act, and Congress also will have a role to play in crafting appropriate regulation. Unfortunately, however, scammers may pay little attention to regulations, so regulators should focus on AI-detection and content authentication guidance, which will enable consumers to identify whether they are seeing or hearing authentic content or AI-generated, and possibly fraudulent, content.

I would like to close with a quick anecdote. Prior to teaching at Bentley University, I taught in the Massachusetts state prison system where one of my students was doing two consecutive life sentences. I told him I always wondered about his experience being sentenced and he replied that he shouted at the judge, "How do you expect me to do two life sentences?," to which the judge replied, "Just do the best you can."

When it comes to protecting seniors from the daunting challenge of AI-enhanced scams, the time is now to do the best we can.