S. HRG. 118–179

MODERN SCAMS: HOW SCAMMERS ARE USING ARTIFICIAL INTELLIGENCE AND HOW WE CAN FIGHT BACK

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING

UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

WASHINGTON, DC

NOVEMBER 16, 2023

Serial No. 118–11

Printed for the use of the Special Committee on Aging

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

54–250 PDF WASHINGTON : 2024

SPECIAL COMMITTEE ON AGING

ROBERT P. CASEY, JR., Pennsylvania, *Chairman*

KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
ELIZABETH WARREN, Massachusetts
MARK KELLY, Arizona
RAPHAEL WARNOCK, Georgia
JOHN FETTERMAN, Pennsylvania

MIKE BRAUN, Indiana
TIM SCOTT, South Carolina
MARCO RUBIO, Florida
RICK SCOTT, Florida
J.D. VANCE, Ohio
PETE RICKETTS, Nebraska

ELIZABETH LETTER, *Majority Staff Director*
MATTHEW SOMMER, *Minority Staff Director*

C O N T E N T S

MODERN SCAMS: HOW SCAMMERS ARE USING ARTIFICIAL INTELLIGENCE AND HOW WE CAN FIGHT BACK

Thursday, November 16, 2023

U.S. SENATE
SPECIAL COMMITTEE ON AGING
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m., Room 106, Dirksen Senate Office Building, Hon. Robert P. Casey, Jr., Chairman of the Committee, presiding.

Present: Senator Casey, Gillibrand, Blumenthal, Warren, Kelly, Braun, and Rick Scott.

OPENING STATEMENT OF SENATOR ROBERT P. CASEY, JR., CHAIRMAN

The CHAIRMAN. The Senate Special Committee on Aging will come to order. We want to thank everyone for being here this morning. Welcome to the Special Committee on Aging's 10th hearing of the 118th Congress.

Today's hearing is entitled, ″Modern Scams, How Scammers are Using Artificial Intelligence and How We Can Fight Back.″ We are here today to discuss fraud and scams, an issue that has touched millions of American families, including, of course, older adults.

In 2022, frauds and scams cost Americans $9 billion, a 30 percent increase from just one year before. Older Americans lose more money to scams on average than younger adults. Last year, they reported losing more than $1.6 billion to fraud, though the actual losses can be as high as $48 billion.

It has long been an Aging Committee priority to protect older adults from fraud and from scams. Today, we are releasing the Committee's 8th annual fraud book. This critical resource captures the most common scams targeting older adults in 2022 and offers resources to protect against fraud. Here is the book, and here is the Spanish version of the book.

We are very proud of the work that goes into this, the staff work by members of the staff on both sides of the Aging Committee, both majority and minority staff. This year, the Committee's work is, among other things, focused on exploring a new threat related to scams. Of course, that is what we know is AI, artificial intelligence.

By now, we have all likely heard of what artificial intelligence is all about, and we have also heard of generative AI, a nascent, vast and opaque tool that many Americans don't fully understand. I would include in that the work that the Senate is doing.

Member, individual members of the Senate, both parties are trying our best to understand artificial intelligence and especially generative artificial intelligence. We are learning as well, and at the same time as the Nation is learning.

While we are working to understand the potential applications of AI, scammers have been integrating it into their schemes to make their employees more lifelike and convincing. Deepfakes or AI developed images that look nearly identical to a real life person and voice clones can mimic the voice of a loved one and can easily dupe consumers and businesses into giving away valuable personal information or money.

Any consumer of any age can fall victim to these highly convincing scams. In preparation for today's hearing, my staff spoke to numerous people around the country who were scammed or nearly scammed by these bad actors using AI.

These stories are heartbreaking, with victim after victim expressing reactions of fear, despair, disbelief, and anger. One of our witnesses will share his story today, Gary Schildhorn. Gary is from Montgomery County, Pennsylvania, just outside of Philadelphia in the Southeastern corner of our State.

Gary will talk about, despite knowing all the signs, talk about his situation of nearly losing $9,000 to a scammer after he heard a voice clone of his son on the other line pleading for help. Gary, I want to thank you for being here today and for telling your story. We will also have a chance to hear from six other people today who are willing to share their stories.

The following will appear in a video, Jennifer DeStefano from the State of Arizona, Amy Conley from the State of New York, Janis Creason from the State of Pennsylvania, Dauphin County, right in the middle of our State, and Terry and Elva Holtzapple and their neighbor, Jake Rothermel, from Potter County, Pennsylvania, way up on the Northern border, the New York border of Pennsylvania.

We will share some of their experiences today and more of their stories will be available on the Aging Committee's website. These stories are awfully hard to hear, and they are tragic. I know that as a parent, I would feel the same fear and the same need to react or act if I heard about—I heard the voice of one of my daughters or something that happened to them, or my grandchildren on the other end of the phone begging for assistance.

Any one of us would react in the ways that the testimony today will outline. This is something we all have to be more aware of, so with that, we are grateful you are here today, but we will play this video clip first, and then I will turn to ranking member Braun.

[Video playing.]

FEMALE SPEAKER. Immediately heard, Mom, I have been in an automobile accident. I have been in an accident.

FEMALE SPEAKER. Immediately I heard sirens and my daughter's voice, and she said in a crying voice, mom, I got in an accident.

MALE SPEAKER. My daughter was—how—she was crying on the phone. I mean, profusely crying and saying, mom, mom, mom, and of course, my wife was saying, Leanne, Leanne, what is the matter? Leanne, Leanne, and then she repeated it again, mom, mom, mom, and it was—it sounded exactly like her.

FEMALE SPEAKER. I answered the phone, and it was my 15 year old daughter crying and sobbing saying, mom, mom, mom, help me. These bad men have me. Help me. Help me. Help me.

FEMALE SPEAKER. Someone called posing as someone from law enforcement—the court system, I would say someone in the court system, and explained to me what had happened, that my daughter had been charged, what the next steps were, and said that they could get her into a program that would ensure she did not get points on her record, that she would not be charged, and said there would be some cost involved to it.

FEMALE SPEAKER. The phone rang right away, and it was someone who said they were from the probation agency and that it would be $15,000 to get her out of jail.

MALE SPEAKER. It wasn't very long, a public defender called. She said, she is going to be charged and she is going to go to jail. She said, but you can post bail for her if you want to, and she won't go to jail. We said, well, how much is the bail? She said, it is $15,000.

FEMALE SPEAKER. He started to demand $1 million. That was impossible. Then he got really angry with me about that, so then he came up with $50,000.

MALE SPEAKER. There was something subconscious about this incident that I believe resonated with them, that things were not all on the up and up.

FEMALE SPEAKER. As I was ready to get in the car, actually to head to the bank and get out money to send with the courier, honestly, I just put my head down in the car and just said a prayer. Out of the blue, it was just like, it is a scam.

FEMALE SPEAKER. She sent a picture of herself at home smiling, saying, I am fine, so at that point, I knew it was a scam.

MALE SPEAKER. Jake called us back. He found out all the information. I was on the phone with him, and Elba was on the phone with Leanne, and Jake said, it is a scam.

FEMALE SPEAKER. Then finally, the mom who was with my daughter, Aubrey, was able to get my husband on the phone who was able to locate my older daughter, Bree. I demanded that I talk to her to make sure that was really her. I started asking her questions, and she is just, mom, I have no idea what is going on. I am here with Dad, and at that point, then that is when I knew that this was a scam.

FEMALE SPEAKER. It is the worst feeling a parent can have.

FEMALE SPEAKER. It has rattled us for sure.

FEMALE SPEAKER. I was devastated when I heard it. I was upset. I had tears.

FEMALE SPEAKER. I could hear in the background pleading and crying and begging for my help, and then that is when I got really scared.

MALE SPEAKER. Scammers are going to basically play on one thing, and that is on the heartstrings of particularly family members, because when it comes to family, we will do anything for our families.

[End of video.]

The CHAIRMAN. Well, you heard it all there. That is what we are dealing with here, and real people in real lives. Ranking Member Braun.

OPENING STATEMENT OF SENATOR MIKE BRAUN, RANKING MEMBER

Senator BRAUN. Thank you, Mr. Chairman. What we just listened to there, it is going to get worse because we are at the leading edge of this technology, and it has always amazed me in running a business for as long as I did, and when we embraced technology 15 to 20 years ago, and it became such an important part of running a profitable, efficient logistics and distribution business, but constantly you have got folks out there through credit card scams, you name it.

They are after everyone, and it amazes me how broad it is. Now you see what happened here. I think the main takeaway is that AI obviously can be used for that. It also may be the tool that you can use against it. That is kind of the conundrum.

We just need to figure it out. Private sector has been using AI, I think beneficially, for a long time. Dates back into the 90's. It is important I think the Government embraces the technology so it understands it, so that we can come up with some paradigm that is in place to help folks like we just listened to.

I am going to be introducing the Medicare Transaction Fraud Prevention Act, which will be very simply for all the fraud that comes around it using the same tools credit card companies have used for a long time, and you have all been part of that, where somehow they get your credit card number. They do a great job at it. In most cases, the fraud does not occur.

There is no reason we wouldn't want to, minimally at least, mimic that. It is going to target two particular areas, diagnostic testing and durable medical equipment. That is another way you can scam—and here you are involving the Government, and these are generally expensive items, medically speaking.

What this would do is notify beneficiaries in real time with suspicious activity. While some of my colleagues have called for a heavy handed Federal approach to AI, I am very concerned that we don't smother it because it is already out there, and the malfeasance is ahead of maybe the good results that can come from it.

I am proud to be part of this hearing. It is very important that we keep this in the discussion mode. Be sure that we don't smother the technology because it is already out there, and if we do not embrace it, we will not be able to counter the ill effects out there. I yield back, Mr. Chairman.

The CHAIRMAN. Thank you, Ranking Member Braun. I will start our witness introductions. I will do three, and then I will turn to Ranking Member Braun for our fourth witness. Our first witness, as I mentioned in my opening, Gary Schildhorn, and Gary, I want to thank you for being here, for telling your story.

Gary is a lawyer in Philadelphia. He specializes in corporate law, including corporate fraud. He will share his experience with a bad actor, and that is a terrible understatement, who used his son's voice to try to scam him out of thousands of dollars, something no parent, no family member wants to endure.

Gary, thank you for being here with us today and for sharing your story. Our second witness is Tom Romanoff. Tom is the Director of the Technology Project at the Bipartisan Policy Center. He has previously led IT initiatives, etcetera, for several Federal agencies and explained the impact of new technology on Government operations.

He will discuss how AI is being used to make fraud and scams both more sophisticated and harder to detect. Mr. Romanoff, thank you for being with us today and bringing your expertise. Our third witness is Steve Weisman, a Professor, Attorney, and an expert in scams, identity theft, and cyber security.

Mr. Weisman has dedicated his career to educating consumers on how to safeguard against fraud and scams. Thank you for being here and for sharing your expertise with us. I will now turn to Ranking Member Braun.

Senator BRAUN. My pleasure to introduce Dr. Tahir Ekin. He is the Field Chair in Business Analytics and Professor of Information Systems at Texas State University. His book, ″Statistics and Health Care Fraud, How to Save Billions,″ covers fraud prevention strategy and many of the trends that will be discussed here today.

Thank you for coming here to testify for us.

The CHAIRMAN. Thanks, Ranking Member Braun. We will turn to our first witness, Gary Schildhorn.

STATEMENT OF GARY SCHILDHORN, JD, ATTORNEY AND INTENDED SCAM VICTIM, PHILADELPHIA, PENNSYLVANIA

Mr. SCHILDHORN. Thank you, Chairman Casey, Ranking Member Braun, for inviting me to this hearing. I hope my testimony is useful. As you mentioned, I am a practicing attorney in Philadelphia, and I was the intended victim of a scam using my son's voice, and here is the story. I was on my way to work.

My phone rang. It was my son. He was crying. He said, dad, I was in an accident. I hit another car being driven by a pregnant woman. My nose is broken. They arrested me. I am in jail. They assigned a public defender to me.

His name is Barry Goldstein. You need to call him. You have to get me out of here. Help me. I said Brett, I will call him, and I will call you right back. He said, you can't. They took my phone. Help me, dad. I am a father. I am a lawyer.

My son is in trouble. A pregnant woman was hurt. He is in jail. I am in action mode. Before I could do anything, my phone rings again. It is Barry Goldstein. I just met with your son. He is hurt. He has a broken nose, but he will be okay.

He hit a car being driven by a pregnant woman. She was taken to the hospital. They arrested your son because he failed the breathalyzer test at the accident scene. I said, wait, my son would never drink and drive.

He said Brett told him that, but he had an energy drink that morning and that may have caused the failed test. He said I should take some steps if I wanted to, to bail my son out. I said, of course I want to do that. He said, well, I will give you the phone number for the courtroom, courthouse, and here is your son's case number.

You should call the courthouse and bail him out. I immediately called the courthouse. They answered correctly. I tell them why I

am calling. They said, what is your son's name? They asked for the case number.

They said, yes, your son is here. Bail was set at $90,000. You need to post 10 percent, $9,000 to bail him out, but there is a problem. I said, what is the problem? The county bail bondsman was away on a family emergency, and he is not available. He said, but there is a solution. You can post what they called an attorney's bond.

I said, I am an attorney. He said, yes, but you haven't entered your appearance on behalf of your son. There is a Mr. Goldstein that did that. You should perhaps call him back and try to get him to post the attorney's bond. I hang up. I call Mr. Goldstein back.

Mr. Goldstein, can you post the bond for my son? Yes. You need to wire me $9,000. He said I am a member of a credit union, so you need to take the cash to a certain kiosk, which will get the money to me, and I am scheduled to leave for a conference in California. I will be leaving to the airport in two hours, so you need to move quickly.

I learned later that that kiosk was a Bitcoin kiosk that would convert the money to cryptocurrency. I hang up. All of these calls happened in two minutes. This is the first time I had a chance to think. I called my daughter-in-law and suggested that she call work and tell them that my son wasn't going to make it today because he was in an accident.

A few minutes later, Facetime call from my son. He is pointing to his nose. He goes, my nose is fine. I am fine. You are being scammed. I sat there in my car. I was physically affected by that. I was—it was shock and anger and relief.

I decided that I would try to keep Mr. Goldstein engaged in the scam while I invited law enforcement to become involved. I contacted the Philadelphia police and they said because I had not lost the money, they couldn't help me. I called the local FBI office.

They said, look, there is burner phones and cryptocurrency. They are aware of this scam, and that they were unable to bring back cryptocurrency once it was out of the country or wherever it went, and so they were unwilling to get involved, and that left me fairly frustrated because I had been involved in consumer fraud cases in my career and I almost fell for this. The only thing I thought I could then do was to warn people. I approached the Philadelphia Inquirer and they did a feature story, and Fox News ran a segment on their morning show.

The scam hasn't abated. Since that article came out, I have received 20 to 25 calls throughout the country of people who have been contacted by Barry Goldstein and who had lost money, and they were devastated.

I mean, they are emotionally and physically hurt. They almost were calling to get a phone call hug because they were so upset. They asked me, you know, what could I recommend? I said, look, the—do what I did.

Go public. The other suggestion I had was to go to the bank where they bank and suggest the tellers inquire about anyone that's taking out a lot of cash that doesn't usually do that. That was the only thing I could come up with.

The cryptocurrency and AI have provided a riskless avenue for fraudsters to take advantage of all of us. They have no risk of exposure. I know that there is economic benefit to cryptocurrency, but I also know that it causes substantial harm to society, and financial harm.

To me, you know, it is fundamental if we are harmed by somebody, there is a remedy either through the legal system or through law enforcement. In this case, there is no remedy, and that fundamental basis is broken, and I hope that this committee could do something about that. Thank you.

The CHAIRMAN. Well, Gary, thanks very much for telling your story. It will help us better be prepared in helping others. Mr. Romanoff, you may begin your opening statement.

STATEMENT OF TOM ROMANOFF, DIRECTOR OF THE TECHNOLOGY PROJECT, BIPARTISAN POLICY CENTER, WASHINGTON, D.C.

Mr. ROMANOFF. Thank you, Chairman Casey and Ranking Member Braun for having me today. It is an honor to be here. Thank you, Gary, for sharing your story with us today. I am Tom Romanoff. I am the Director of the Technology Project at Bipartisan Policy Center, where we focus on bipartisan solutions for the technology sector. We started this work in 2019 when we formulated the AI National Strategy with representatives Will Hurd and Robin Kelly.

The strategy passed as 1250, House Resolution 1250, alongside seven other bipartisan sponsors. Prior to my role at the Bipartisan Policy Center, as you mentioned, I advised C-suite executives on emerging technologies and policy, and included in my clients were the Office of Management and Budget, the FDA, General Services, among many others.

There are a lot of questions about what this technology can do and what it cannot do, so I want to first level set about generative AI.

First, we are speaking about a very specific type of AI. There are six other disciplines, all of which profoundly impact our world. We are seeing exponential growth across all of those disciplines and branches of AI.

Second, many of the ideas we are discussing today predate AI's current use and current capacity. The use of AI to amplify these crimes is concerning as we already know the challenges in stemming scams and frauds were difficult before the capability of AI was brought to bear.

Third, last year, publicly available generative AI programs got so good at—that most people could not tell the difference between computer generated content and human generated content.

With the recent capacity enhancements and this technology's availability, cybercriminals are increasingly adopting it. Generative AI specifically poses some questions because it has compounding effects beyond what we have seen to date. Number one, it makes it easier, cheaper, and faster for scammers to produce deceptive content, and number two, the increasing quality, quantity, and targeting capabilities lend a hand to fraud. It is critical to understand that while AI has numerous benefits, its misuse in scams is a

growing concern. Adding to said concerns is that cybercrimes are on the rise.

As you mentioned earlier, the Federal Trade Commission reported that a staggering steady increase of online fraud losses year over year has been increasing, with 2022 losses reaching around $9 billion.

Addressing this challenge requires a multi-pronged approach, especially in the age of AI. We need to enhance synthetic media detection capabilities, ensure content verification, develop standards and response processes, and implement multiple authentication factors for users, while addressing issues in the defense mechanisms themselves, such as bias and discrimination in the automation detection systems.

On that last point, please don't make any mistake. The use of AI models with biased data to detect cyber fraud detection may have significant consequences. AI is just a model that uses data, and we never really figured out the data considerations, and so the AI models will have the same questions and concerns that we have around data use and decisionmaking that we have been asking ourselves for 20 years.

If AI systems are fed garbage data, then they will produce garbage outcomes. In closing, the pace at which AI is being adopted and advancing is breathtaking. As we embrace its benefits, we must also be vigilant against its risks, especially cybercrimes.

The recent Executive Order by President Biden emphasizing the management of synthetic content and labeling a verification of AI generated media is a step in the right direction. However, more concentrated efforts are needed at both the Federal and State levels, and the role of Congress cannot be understated.

We must codify and standardize the undefined aspects of this technology in order to respond to the negative use cases. States will continue to forge ahead with their own laws and regulations, creating a patchwork of definitions, standards, and enforcement that could be further exploited by cyber criminals.

It is often said that innovation is at the heart of progress, but it is critical that Congress works to strike a balance between innovation and regulation to safeguard our society, particularly our senior citizens, from the dark side of AI. Thank you.

The CHAIRMAN. Thank you, Mr. Romanoff. Mr. Weisman.

STATEMENT OF STEVE WEISMAN, JD, SCAM EXPERT, EDITOR OF SCAMICIDE.COM, SENIOR LECTURER, BENTLEY UNIVERSITY, WALTHAM, MASSACHUSETTS

Mr. WEISMAN. Chairman Casey, Ranking Member Braun, thank you for the opportunity to provide testimony today.

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 developments, and tips on how to avoid these problems.

Scamicide was named by the New York Times as one of the three best sources for information about Covid related scams. When it comes to fraud and scams affecting seniors, I am here to tell you things aren't as bad as you think.

Unfortunately, they are far worse. According to the FTC's Consumer Sentinel Report, which was just released a few weeks ago and you mentioned, older Americans reportedly lost $1.6 billion to frauds and scams in 2022.

As you also mentioned, 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.

The FTC estimates in 2022 the actual amount lost by seniors could be as high as $48.4 billion. Now, with artificial intelligence, the scams are getting worse. AI has become a sophisticated weapon that can be effectively utilized by even the most unsophisticated scammers.

Today, I would like to tell you about a few of the scams in which AI is being used and how we can protect older adults. By now, as you heard, many people are somewhat familiar with the family emergency scam or grandparent scam in which a family member receives a telephone call from someone posing as their loved one.

The individual on the phone claims to have gotten into some trouble, most commonly a traffic accident. In grandparent scams, the scammer pleads for the grandparent to send the money immediately to help resolve the problem and begs the grandparent not to tell mom and dad.

Now, this scam has been perpetrated for approximately 14 years, but it is getting worse, and we have AI to thank for that. Through the use of readily available AI voice cloning technology, a scammer using a recording of the grandchild or child's voice obtained from YouTube, Tik Tok, Instagram, or voice mail can create a call to the grandparent that sounds exactly like the grandchild.

All it takes is AI voice generating software readily available and as little as 30 seconds of audio. Phishing emails, and the more specifically targeted spear phishing emails, use social engineering to lure the targeted victim to click on a link, download a malware attachment, make a payment, or provide personal information.

Spear phishing, however, is a personalized phishing email that incorporates information about the targeted victim to make that email more believable, and phishing is used in a variety of schemes. In 2021, Google conducted a study in conjunction with researchers at Stanford.

The researchers studied more than a billion malicious emails targeting Gmail users, and they found that the number of phishing and spear phishing emails users received totaled more than 100 million each day.

Again, as bad as a threat as socially engineered spear phishing emails have presented in the past, they are far worse now because of AI. Using AI, scammers can create more sophisticated and effective spear phishing emails that are more likely to convince a victim to fall for a scam.

In the past, phishing emails, particularly those originating overseas in countries where English is not the primary language, could be recognized by their lack of grammar, syntax, or spelling. However, AI has solved those problems for foreign scammers and their phishing emails are now more difficult to recognize.

So how do we protect seniors from scams? Well, 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, and this committee has also done this through publications such as its Fraud Book publication, which contains much useful information.

Fortunately, AI can also be an effective tool in combating AI enhanced scams. Machine learning algorithms can analyze vast amounts of data to identify patterns and trends associated with spear phishing emails.

AI can also be used to identify robocall patterns and detect spoofing, a technique used to manipulate caller ID and mimic another phone number. Regulation of AI is critical to protecting people from AI enhanced scams, and as was said, the President's recent Executive Order is a promising first step.

The FTC has regulatory authority over AI through Section five of the FTC Act, but Congress will also have a role to play in crafting appropriate regulations. Unfortunately, scammers may pay little attention to regulators, so regulators should focus on ensuring consumers can identify and authenticate content.

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

The CHAIRMAN. Thank you, Mr. Weisman. Dr. Ekin. Is that—did I pronounce that correctly, Ekin?

STATEMENT OF TAHIR EKIN, PH.D, PROFESSOR AND DIRECTOR OF THE CENTER FOR ANALYTICS AND DATA SCIENCE, TEXAS STATE UNIVERSITY, SAN MARCOS, TEXAS

Dr. EKIN. You did. Thank you, Chairman Casey and Ranking Member Braun. Today, as we convene, it is alarming to acknowledge an 81 percent increase in losses to scams among older Americans, accounting to billions of dollars in the past year.

I am Tahir Ekin, Fields Chair in Business Analytics and a Professor at McCoy College of Business, Texas State University. My research dives into the critical intersection of AI and fraud detection. I am honored to testify on this urgent matter today.

Scams continue to affect older Americans at alarming rates. Despite improved awareness and educational campaigns, both the losses and the number of victims has surged. This prompts the question, are scammers becoming more sophisticated or our response is lagging?

The reality likely involves a combination of both. AI amplifies the impact of scams, enhancing their believability and emotional appeal through personalization. Voice and face manipulation illicit urgency and familiarity, manipulating older adults' emotional responses and vulnerability. Notably, there is a surge in personalized scams.

Recognizing the growing role of AI in scams is crucial. While efforts to help scammers are underway, we should also explore AI as part of the solution. My research centers on AI methods for health care fraud detection draws parallels to combating scams targeting older Americans.

Industries like credit card companies have successfully used AI for fraud detection, denying suspicious transactions in almost real

time, and collaborating with consumers for confirmation. However, health care fraud still incur substantial losses as high as 10 percent of our annual health expenditures, which could mean more than $300 billion.

Hence the name of my book, ″Statistics on Health Care Fraud, How to Save Billions.″ We have limited resources to analyze billions of transactions. Statistics and AI find the needle in the haystack to support the auditors and save taxpayers money.

AI's proactive role extends to monitoring online platforms and blocking potential scam calls, yet its true potential lies in collaboration as seen in Government health care programs. Initiatives like the Medicare Transaction Fraud Prevention Act that advocate data collection and call verification with beneficiaries are essential for AI integration, akin to credit card fraud detection.

Responsible AI methods can facilitate personalized education campaigns while preserving privacy and ethics. For example, AI can flag a typical behavioral patterns like sudden financial transactions, enabling tailored alerts and educational materials for older adults. Last, fraudsters are adaptive, and scams will evolve.

Use of adversarial AI can help proactively limit scammers' abilities. Acknowledging AI's imperfections such as false positives and addressing privacy concerns is crucial. However, by constructing responsible AI systems, we can empower older Americans while navigating potential risks.

To effectively combat these evolving threats, collaboration among Government agencies, tech companies, financial institutions, and consumer advocacy groups is crucial. Sharing insights and data to train these AI models to detect and prevent these scams is pivotal, including input from older adults in developing AI driven tools is also necessary.

In the fight against AI driven scams, awareness and AI literacy are critical weapons. Existing efforts, such as the President's campaign, can be enhanced to include AI related steps. In the context of ethical use of AI against scams, clear disclosure of the use of AI in communication, marketing, and financial transactions, with a focus on protecting vulnerable populations is important.

Accessible support and reporting mechanisms such as the toll free for all hotline are crucial against gaps. AI based chat bots and communication channels can supplement and provide additional support outside the business hours and at the time of need.

AI also can make public scam campaigns more impactful, making them tailored to the needs of specific older adult groups. In conclusion, the interplay of AI and scamps brings forth challenges and opportunities.

Striking a careful balance between fostering AI innovation and protecting vulnerable populations is paramount. I advocate for proactive and personalized AI based supporting measures, recognizing the difficulty in recovering both lost finances and mental well-being after a scam has occurred.

By prioritizing the enhancement of their data and AI literacy, we can also actively involve older Americans in prevention and detection. Understanding the impacts of dynamic disruptions like AI will undoubtedly take time.

As a realistic optimist, I find hope in the collaborative efforts to yield robust and trustworthy AI applications, fostering a safer environment for older adults. Thank you for providing this platform to address this critical issue.

Your work in safeguarding older Americans against scams and raising awareness is commendable. I eagerly welcome any questions or discussions the committee may have. Thank you.

The CHAIRMAN. Doctor, thank you very much. We will now move to our questions of the witnesses, and just for folks' awareness, today is Thursday, so we have Senators in and out coming from other hearings and other commitments, so we should have some Senators here at 10:45.

It will be about the time that Senator Braun and I are probably through our first round of questions. I will start with Gary Schildhorn. Gary, thanks again for sharing your experience, and we know that when it comes to these scams, these bad actors, or better way to refer to them as criminals, will prey upon our vulnerabilities and our fear. They know we are human beings.

They know they can advance their scam by playing on those fears and those vulnerabilities. With artificial intelligence, scammers can more easily and quickly and accurately tailor or target their scams to intended victims.

The Committee offers resources, including the Fraud Book which I mentioned earlier, that shares some red flags to watch out for and steps to take to prevent against scams. We are also releasing a brochure, which I have here, that will provide more information in a shorter form.

Gary, I wanted to ask you this. Why do you think people should—what do you think people should know about AI assisted scams, number one, what should they know? How should they identify them? What are some of the red flags or indicators that you have learned since you were the target of this?

Mr. SCHILDHORN. Thank you for the question. It is very difficult now to see red flags. The person that I spoke with, Barry Goldstein, spoke coherent, intelligent English. There were no grammatical errors or mispronunciation of words. His text messages back and forth were clear and responsive.

When I was engaging him to, while I was trying to get law enforcement in, I told him that I was trying to find this name in Martindale Hubbell, and for lawyers, that is where lawyer biographies are found. He sent me a biography that he had already had ready.

It is very difficult for that—for you to see a sign that it is a scam. There is one way that I recognize as a red flag. When someone is asking you to send money either by cash or by gift cards or other untraceable methods, that is the red flag.

That is when an antenna should go up and say, well, why aren't they just asking me to do a regular wire transfer from my bank to their bank? In answer to your question, that is the main red flag that I see that a consumer could react to as a possible indication of a scam.

The CHAIRMAN. I know that over the years and among other things that our Fraud Book has talked about, just in the context

of certain kinds of scams, that there are red flags. I understand what you are saying, they are a lot harder to detect.

For example, we used to say that, and it is still the case with these IRS scams that are somewhat related to what we are talking about, but now of greater sophistication, but the rule, one rule was, if someone calls you and says they are from the IRS on the telephone, it is your first contact, it is not the IRS. You always get something in writing.

I realize that is a rather simple rule. Much harder to find the simple red flags with the sophistication of AI. Mr. Weisman, I know you have got a website, scamicide, which features a tremendous amount of information about scams.

You have been doing this for about 12 years, a scam of the day, and it is hard to believe you have that much content, but that tells you the gravity of the problem or the scope of it. Your work demonstrates how pervasive and persistent scammers are and how diverse their tactics are when targeting witnesses.

This Committee has been collecting data on scams targeting older adults for about 10 years now. We have seen trends that change and new technologies that emerge, and obviously some of those are set forth in the Fraud Book.

In the time that you have been running—operating the website, how have you seen technology change and tactics shift? Maybe, what is your advice for us as we look forward down the road, especially with the advent of AI?

Mr. WEISMAN. You mentioned when I started scamicide, I wondered if I would have enough scams to do a new one every day, and after more than 4,400 scams, unfortunately they don't stop. You know, the scams—the scams have been with us forever.

The Nigerian email is just an update of a scam called the Spanish Prisoner from the 1500's, and the cryptocurrency scams we see, even cryptocurrency pump and dumps were done before.

You are right, the technology has changed it. It has changed the delivery systems as far as robo calls. It is done it—the voice over internet protocol where phones can be—messages can come in from all over the world over a computer, and the phone is still the way that seniors get the most scammed.

Then there is even something called spoofing. You mentioned the IRS, and you know it is not the IRS, which is the same line I have always told people. However, they look at their caller ID and they see the call is coming from the IRS, and so they trust it. That is where my motto comes in is, trust me, you can't trust anyone.

AI has just enhanced that, and sort of what Tom was saying, any time you are asked for personal information, any time you are asked to make a payment of any kind, any time you are asked to click on a link, you have got to be skeptical. You have got to hold back and check it out.

That is a nice rule that can be very difficult when these scammers, the scam artists, the only criminals we call artists, have a knowledge of psychology Freud would have envied and they are able to manipulate us, and that is where we need to change our minds.

The CHAIRMAN. Thanks very much. Ranking Member Braun.

Senator BRAUN. Thank you, Mr. Chairman. Mr. Schildhorn, how did the story end with Barry Goldstein? I see where he actually got mad at you at the tail end. Was anybody ever able to track this guy down, or is he still out there?

Mr. SCHILDHORN. Ranking Member Braun, it ended when I asked him for his Social Security number.

Senator BRAUN. I see that, yes.

Mr. SCHILDHORN. He told me—he actually cursed me out. Told me I didn't love my son and stopped communicating with me at that point. That is how it ended. What was the second part of your question?

Senator BRAUN. In other words, he got frustrated and then he just disappeared into the ether then?

Mr. SCHILDHORN. He recognized that, but is he still out there? Yes. I know that because the calls I got when people found my article were telling me that it was Mr. Goldstein.

Senator BRAUN. He is still using the same name?

Mr. SCHILDHORN. It works. Why not? When the reporter reached out to him, it was pretty incredible because the reporter said, you are in California. How did you meet with Schildhorn in Philadelphia? Oh, well, it was a phone meeting. I mean, he had answers for everything. Yes, as far as I know from the calls I have received, that scam is unabated. It still goes on, and no one has——

Senator BRAUN. The traceability of using a phone or whatever he does has never led authorities to Mr. Goldstein?

Mr. SCHILDHORN. When I first contacted the FBI, they said, well, they use burner phones which cannot be traced, and the cryptocurrency cannot be recalled. At that time, I am not even sure they could find the accounts that cryptocurrency—this was 2020, so law enforcement had no solution.

As I said in my testimony, it is fundamental in our system that if you are harmed, you have a remedy. Here, there seemed to be no remedy, neither the courts of law or law enforcement.

Senator BRAUN. He is not the only one. Thank you for explaining that thoroughly. Question for Mr. Romanoff. When you look at how AI has been used in terms of credit card companies, health care, we know, and we have seen some real graphic examples of how it is used maliciously. Can you go over a few of the things that we know it has worked at and saved time and money?

Mr. ROMANOFF. Yes. The sheer amount of information and data that needs to be processed in order to protect systems against cybercrime and hacking is—a human can't do it, and so, there is algorithms that have existed for many years now.

AI has been used to assist cyber defenders for years in terms of processing that information, identifying trends, and flagging anything that could be fraudulent in that space. That continues to be a major factor in terms of defending against some of these attacks.

In terms of, you know, some of the expanded capacity of being able to detect whether a phone call is actually coming from the right person or identifying trends in robo calling and things like that, AI can be very useful in assisting in that, which does tend to stem some of the scams that are being perpetuated.

In terms of, you know, direct correlation between what the credit card companies and this application—you know, there are some ob-

stacles there. You have to have the credit card company, or a financial institution involved in order to, you know, identify a fraud or scam, so when it is happening at an individual level, there is some question as to who steps in and uses these powerful systems to identify that.

Senator BRAUN. In your opinion then, for the bill that we are introducing, I am going to—I think I am going to get colleagues on the other side of the aisle, the Medicare Transaction Fraud Prevention Act, which is aimed at diagnostic testing and durable medical equipment.

Is there any reason the principles of what you just described wouldn't work to prevent fraud there, you know, through CMS?

Mr. ROMANOFF. Well, the first thing that comes to mind is that there is different data regulations in terms of HIPAA versus consumer data and protections on that front. I would have to read the bill in order to provide specific insights on that. In terms of the systems of AI being used to identify fraud, you can see an application there, in the application of health care in general, yes.

Senator BRAUN. That amount, by the way, is $60 billion a year.

Mr. ROMANOFF. Oh, yes.

Senator BRAUN. Defrauding Medicare. It is a lot. I got another question. Do you want to yield back and——

The CHAIRMAN. Go ahead. Go ahead.

Senator BRAUN. Okay. This is for Dr. Ekin. We just described what was happening in our own Government. Like when we did the extended unemployment benefits, which was just under $1 trillion, and there is an estimate that anywhere from $100 to $200 billion from domestic and foreign fraudsters.

When the Government is involved, it is like, you know—it is a lot easier, seemingly, to defraud. I have never heard commercial entities—they have got all this protective gear. Here, you know, it is like picking it out of a toddler's hand almost.

What can we do here and what do you—let's just look at, CMS's current Medicare fraud prevention system. Compare it to what could be out there, and is it any different from what it was years ago?

Dr. EKIN. Thank you, Senator Braun, for the question. There have been many improvements actually. In 2011, basically since 2011 now CMS has authority to use predictive algorithms to identify fraud, and they have come up with this fraud prevention system, and now we have the second installment of that.

Over time, they have been using some both prepayment and post payment methods to detect fraud. Most of the focus has been on post payments, which basically focuses on more pay and chase transactions, so basically the system pays the providers, including fraudsters, and then try to chase the potential—basically funds from the fraudulent transactions, which we are not as successful. We are not able to recover as much.

Recently, with the second basic installment of the fraud prevention system, they also added prepayment edits, but they mostly focus on basically eligibility of billings with respect to the policies and rules of Medicare.

Senator BRAUN. Is the amount of $60 billion a year going down, or is it still going up?

Dr. EKIN. I believe it is still going up because also annual health care expenditure saving going up, right, in the—specially the last decade. Most of the Government agencies overall lost around three to ten percent, given that we are spending more than $4 trillion on health care. The amount is easily in——

Senator BRAUN. That is all in the context. Currently, we are borrowing $1 trillion every six months to run this business here. When you have got that kind of fraud nipping at its flanks, something has got to give. Yield back.

The CHAIRMAN. Thank you, Ranking Member Braun. We are now joined by Senator Blumenthal.

Senator BLUMENTHAL. Thanks, Mr. Chairman, and thank you for having this hearing on artificial intelligence, which is growing in importance and gaining public attention at an accelerating rate, almost as fast and accelerating rate as artificial intelligence itself is progressing.

As you know, we have done a lot here in the Senate. Majority Leader Schumer has held a number of forums. The subcommittee that I had, a subcommittee of the Judiciary called Privacy, Technology, and the Law has held a number of hearings as well. Ours have been public.

At one of them, I—as a matter of fact, the first I played a recording of my voice and introduced it by saying, now for some introductory remarks. It was my voice, but it was taken from speeches that I gave on the floor of the Senate, and the content of what was said came from ChatGPT.

One of the witnesses at the hearing was Sam Altman of OpenAI. It was literally my voice, content that could have easily been mistaken for something I said. It sounded exactly like what the chairman of a subcommittee would have said, and it sounded exactly like my voice.

Which leads to one of the areas that I think all of you have mentioned, particularly Mr. Romanoff, the impersonation and deepfake dangers. You mentioned in your testimony that some banks now use voice identification to authenticate account ownership because some of the scammers are using voice impersonation in effect to break the authentication that the banks try to use.

Can you talk a little bit about how multiple authentication, which you mentioned in your testimony, can help prevent these kind of scams. Whether they would have any application to the individual senior citizen who gets a call. Sounds exactly like that person's nephew stranded here in Topeka.

I have no money, please wire money. You know the standard fraud, but the impersonation of the voice is used to trick. Might be anyone, not just a senior citizen, but can you talk a little bit about authentication as a means of breaking the potential impersonation scams.

Mr. ROMANOFF. Sure thing. In terms of voice cloning, it is a technology that has been around for a little bit. 1998 was the first time someone cloned their voice using a computer.

With generative AI, as we are all aware, there has been much more capacity and much more availability to access these voice cloning tools. At the same time, banks are, you know, want to pro-

vide services to their customers with an ease of use while protecting their assets.

For a little while, voice banking was something that you could use the biometric markers of a person's voice in order to authenticate them as a user. It was very recently that a reporter was able to break into their own account using voice banking and demonstrate that these—this technology has advanced to the point where it may not be essentially viable in terms of authenticating a user.

In cybersecurity, you are supposed to have multifactor authentication at all times. It does create obstacles to access some of your assets or information or whatever it might be, because the ease of use in terms of doing more than one way to authenticate, you know, can cause people to not want to do that service or whatever it might be.

It is necessary because no longer are voice biometrics enough to it indicate a user. You are seeing banks move away from that or shy away from voice authentication as a way to verify. The second thing is behavioral.

When it comes to cyber hygiene, we tend to engage our products or services in a way that is familiar to us. If you introduce a behavior such as using your voice to authenticate your bank account, then folks that get used to that will be—will expect that, and scammers know that, so they will look for ways that they can capitalize on established behaviors such as voice cloning and voice authentication to access assets.

The second thing is to, as Chairman Casey mentioned, if IRS is calling you and it is the first time you are hearing from them, then that is a red flag. It should also be a red flag if your bank is calling you, because there should be more than one way to authenticate that the bank is the one that is calling you in that space.

I think the main obstacle here is that, you know, you are dealing with an institution when it comes to banks and trying to authenticate versus you are dealing with a psychological attack, in the case of these scams, where the precedent—where the emphasis is on action.

What I encourage folks to do, and this is a very low tech way of addressing the issue, is doing a password among your friends and family and making sure that you are not publicizing that password or putting it in email because hackers will be able to get access to that. If somebody were to call you, you can say password, authenticate.

If they aren't able to do that, then you are probably dealing with somebody who is cloning the voice. That is a very low key way of doing it. When it comes to institutional approaches, a multifactor authentication is probably the best bet going forward.

Senator BLUMENTHAL. How about the individual, you know, living at home. Is there a way and will there be ways—I assume this technology is also developing the authentication, multiple factor technology.

For me, sitting in my living room, getting a call from one of my children, sounds exactly like one of my children saying, you know, I can't talk here at, you know, a bus terminal or train station. I

need money, please wire it. A lot of people fall for that kind of scam.

Mr. ROMANOFF. Yes. I am aware of some use cases where private sector is using AI and technology to try to cut down on robo calling, and it is using some of the technology to authenticate a user that is coming in.

I am not sure if that is—that product or those products are being applied to authenticate voices per se. I can't answer if there is a specific product or process out there for that.

Senator BLUMENTHAL. Thank you. Thank you to all the witnesses who are here today. Thanks, Mr. Chairman.

The CHAIRMAN. Thanks, Senator Blumenthal. We will turn next to Senator Warren.

Senator WARREN. Thank you. Thank you, Mr. Chairman and Ranking Member Braun for holding this hearing. Thank you all for being here. Really important topic. Crypto is a favorite for those who are looking to defraud consumers.

According to the FBI, in 2022, crypto scams were the leading cause of investment fraud in the United States. Using crypto, fraudsters stole a record $2.5 billion from consumers. Crypto fraud isn't hitting all consumers equally. Last year we saw a 350 percent increase in crypto investment scams targeting seniors.

That is the biggest spike among all age groups. That ended up to more than $1 billion that seniors lost in crypto scams. Many victims don't report their experiences, as some of you have noted, out of shame or fear, that billion dollar figure is almost surely an underestimate.

Now, Mr. Weisman, you are a nationally recognized expert on scams and cyber security. Why are older Americans particularly vulnerable to crypto scams?

Mr. WEISMAN. You know, it is older Americans are—they are susceptible generally because there is a part of our—you know, anecdotally we say, well, we have lost a little bit of the fastball, which I can attribute to it. It is not going as far, but there is a part of our brain dealing with skepticism that becomes less viable as we age.

There have been studies done at Cornell, as well as the University of Iowa, that has shown this. Then you get into the issue of cryptocurrencies itself, and there is this fear of missing out. It is, oh my goodness, this is going to be the best thing since the proverbial sliced bread.

The seniors are susceptible to this, but it is even worse than that, Senator Warren, in the sense that when a scammer will scam someone with a cryptocurrency scam, and there are myriads of them, from phony cryptos to using it as the funds that are in various other kinds of investment scams, they become scammed and then they give the list of the scammers, the scammers do, of their victims to other scammers who will contact the victims and say, we are from the Federal Government, we are from the Justice Department, and for a fee, apparently the Justice Department now charges fees, we will collect for you.

They lose again. Fear and greed are two elements that are found in every kind of scam. Unfortunately, crypto just has captured the

imagination of many people, particularly seniors, and it is coming back to bite us.

Senator WARREN. Well, I really appreciate your work on this. You know, as you said, crypto is used in all kinds of scams. Scammers claim to have embarrassing information about someone they will reveal unless the person forks over a crypto ransom.

Scammers pose as friends and loved ones to encourage people to invest their life savings so long as the payment is in crypto. We now understand that scammers even set up fake investment platforms to trick people into buying crypto, that of course they will never be able to get their money out of. I am sorry, go ahead, Mr. Weisman——

Mr. WEISMAN. No, it is—because I think you are—my favorite was on YouTube, there was an investment scam that was going to couple cryptocurrencies and AI. AI is going to show you how to make and the guaranteed millions from crypto and the CEO of the company was there touting it.

The CEO, wasn't real. He was an AI generated avatar and anyone that put money into this thing lost it. It is scary the combination of AI and crypto, and with the anonymity of crypto, that is why the scammers love it so much.

Senator WARREN. Right. Well, so talk for just a second, why crypto? Why is it happening through crypto rather than, say, your bank account or some other transaction account?

Mr. WEISMAN. It is the new shiny object. It is catching our mind, and we think that there is something there. I can't help believe that to a certain extent it is the Emperor's New Clothes. Cryptocurrencies are legitimate, but the idea as making millions in investments on this——

Senator WARREN. It is the new shiny object. Anything else about crypto? The anonymity?

Mr. WEISMAN. The anonymity is terrific. That is one thing, you have people looking for the privacy. Then of course, that is something with crypto mixers where your account gets mixed in with others and becomes very difficult to trace.

One of the things the Government did a great job was after the ransomware attack with Colonial Pipeline, they were able to trace those accounts and get it back, but once it goes into the mixers, then you have got problems.

Now, there is legitimate privacy concerns some people may have, but it doesn't come anywhere near to the scammers.

Senator WARREN. Right. It also, as I understand it, it is fast, so the money is gone.

Mr. WEISMAN. That is the thing. You react—in scams, it is often, you got to act now. It is an emergency. We act immediately, and then I have actually had clients who have been scammed with a credit card fraud and managed to call and stop it. That isn't happening with crypto.

Senator WARREN. Yes and can't—yes. Look, I think that Americans are getting sick and tired of these crypto crimes, and it is long past time that we got some regulation in place to deal with this, and that is why Senator Roger Marshall and I have introduced our bipartisan Digital Asset Anti-Money Laundering Act. This bill has

the support of 14 other Senators, both Democrats and Republicans, and the chair of our committee here. It is endorsed by the AARP.

It would make it easier for financial regulators to track suspicious crypto activity and shut down scammers. I know I am over time, but so let's do this one, and we can do it as a yes no. Mr. Weisman, would crypto legislation like ours help cut down on crypto scams?

Mr. WEISMAN. Yes, absolutely. I love it. Here is the thing. My students at Bentley University were recently studying money laundering and we were talking about this very thing. The law is always behind technology.

The banks have the know your customer rule, which helps. You need to have the private sector and the Government working together. This is—your legislation is long overdue. It is a no brainer in the sense—not that you are a no brainer.

Senator WARREN. No, I take that as a compliment.

Mr. WEISMAN. It is something that absolutely would help immeasurably.

Senator WARREN. Good. Thank you very much. I appreciate it. We have got no time to waste on this. These scams are happening every day. Thank you. Thank you, Mr. Chairman.

Senator BLUMENTHAL. Thank you, Senator Warren. Senator Kelly.

Senator KELLY. Thank you, Mr. Chairman. I want to thank you for the video that you showed at the top of the hearing that told the story of Jennifer DeStefano. Jennifer is a mom of four from Scottsdale. I think we heard earlier, this year she got a call from an unknown number, and when she picked it up, it was her 15 year old daughter. Her daughter was crying and calling out for her. The man got on the phone and threatened to harm her kid unless she paid $50,000. The man said he needed the money in cash and would be coming to her in a van, and folks nearby called 9–1–1, as well as calling Jennifer's husband.

Turned out that her daughter was just at home, not with kidnapers, and the call wasn't real. You know, scammers had used in this case AI to create a voice that sounded like her daughter's voice, and she couldn't tell the difference.

Even though in that moment of extreme, horrific, you know, terror, probably shook Jennifer to her core, the police said there was nothing that they could do. No money was transferred. No crime they said had been committed.

Now, this feels to me, and I imagine many others, and to many Americans, as a huge blind spot in the law. I think we have a couple of lawyers on the panel here. Mr. Schildhorn and Mr. Weisman, how should we in Congress be looking at filling these gaps in the law?

Mr. SCHILDHORN. Thank you, Senator. As I think you have just mentioned as part of your question, it is a fundamental principle of our system that there is a remedy if you are harmed.

And with crypto and AI the law enforcement does not have a remedy and neither does the judicial system. You can't find anyone to sue, so my answer is that there needs to be some legislation that allows these people to be identified or where that money has gone

to be identified, so that there is a remedy for the harm that's being caused.

Currently, there is a hole in the system. There is no remedy that I am aware of.

Senator KELLY. Well, how about the issue that in this specific case—and by the way, I have had this happen to somebody I am rather close with.

Almost the exact same thing, and again, no money was transferred. It was incredibly, you know, shocking to—in this case, it was a grandparent that had the same issue, same thing happened to them with a grandkid.

No money was transferred. To me, that still seems like a crime, attempting to rip somebody off even though they weren't successful. Do you feel we should make that a crime and there are criminal penalties?

Mr. SCHILDHORN. Senator Kelly, I am not an expert on this, but I am a lawyer, so that has never stopped me from giving an opinion.

In this instance, I mean, there are analogies in the law to intentional infliction of emotional distress. I believe that is a cause of action in many states.

There might be a way to enhance that type of a law, that if someone is using this, even if you don't spend money, and you cause that kind of shock and distress, that the law allows you to recover a sum of money that is not calculated by how much you have actually lost, but how much pain and suffering you have incurred because you have been subject to that type of extortion.

Senator KELLY. Mr. Wiseman.

Mr. WEISMAN. Yes. I think Gary hit on the key word there. Extortion is a crime. Attempted extortion is a crime. I do think it already is a criminal violation. I agree with you. I think that some Federal legislation to this particular medium of delivery of this extortion could be done.

The other thing is, one thing I tell my students when we are talking about white collar crime, the answer to every question is, it is about the money, and so here, as has been said before, it is very difficult to trace it. They are using burner phones. Who knows even where they may be.

They may be even using voice cloning technology. They can be in a foreign country where their accents are no longer going to be able to be heard. What we can do is, as the Senior Safe Act is, go after gift card because they pay by gift cards, go after the wiring, go after the banking so you stop it there where people—they are in the rush of emotion.

Then they go to pay by a gift card, and the gift card people say, where is this going? What is this for? They recognize the scam, so stop it before it actually occurs.

Senator KELLY. Thank you. Mr. Chairman, I am going to submit a couple of questions for the record. Thank you.

The CHAIRMAN. Thank you, Senator Kelly. We will turn next to Senator Gillibrand.

Senator GILLIBRAND. Thank you so much for being here. I, like many of the Senators here, have heard so many reports about how

our seniors are being targeted with financial fraud, financial scams, AI generated scams, cryptocurrency related scams.

It is unbelievable the amount that criminal networks, worldwide criminal networks are targeting our older Americans. They have retirement funds, they have life savings, and these times are very complex, and these scams are getting more and more sophisticated. Unfortunately, our older Americans are soft targets for these very, very sophisticated criminal networks.

Let's address AI. Scammers can use AI generated and power technology to do deepfakes on voice, do deepfakes on photographs. We know of a New Yorker whose mother received a call from a scammer using voice cloning AI to mimic her distressed child in need of $50,000 to get her out of jail.

Unfortunately, that scam worked. Mr. Romanoff, are the technology development practices in applying AI that also protect consumers from fraud? Are there any unintended consequences of using AI for this purpose?

Do you believe that the existing Federal agencies are properly equipped, both in their technical capability and congressional appropriations, to combat these targeted scams?

Mr. ROMANOFF. Thank you for that question. I will start with the latter question. Federal—some Federal agencies that are more geared toward law enforcement would be better equipped to deal with these scams.

I do think that generative AI in terms of its uses to perpetuate fraud goes across multiple jurisdictions. There is a need to increase the AI readiness and workforce—in the workforce of AI in the Federal Government.

The folks that can identify these issues and use AI itself to detect the fraud. In terms of your first question—and please repeat, what was it? I am sorry.

Senator GILLIBRAND. It was—well, you already answered it. If you can use AI for good and bad in this scenario. The second was, do the Federal agencies have enough law enforcement power to actually address the problem?

Mr. ROMANOFF. Yes. In both of those scenarios, yes, you can use it for good and bad. I think the consideration around AI and its use to detect fraud is, there is a growing concern right now that, you know, do you invest in the AI systems to detect fraud or do you invest in the workforce, individuals who have the expertise to identify trends themselves?

I think as technology continues to be—kind of expand and adopted, we are going to look at a gap between the folks that are entry level kind of law enforcement folks and the folks that are looking at these systems long term, so there needs to be some sort of consideration around, you know, how do you train individuals beyond using an AI to identify these issues, because data has a deteriorating value over time.

These AI models that are used to detect fraud and train to detect fraud, they need a constant source of data and updates in order to figure out what the latest trend is on that.

Senator GILLIBRAND. Thank you. I only have a minute. Got to do another question. The second question I have is about cryptocurrency.

We have seen the lack of regulation in cryptocurrency being an impediment to protecting consumers. I am very frustrated that the Senate has not held substantial hearings yet on how we can actually provide commonsense, thoughtful regulation to keep good actors in the United States and to have law enforcement tools to ban bad actors.

We have an example where our Attorney General filed a claim against a cryptocurrency company defrauding hundreds of thousands of investors, but one older woman, for example, a retired 73 year old grandmother, invested her husband's life savings of $200,000 in a scam crypto agency—a scam crypto currency company.

We need companies to register with the SEC, with the CFTC, with the IRS. We need oversight by the Fed. We need oversight by all the regulatory organizations, and Congress isn't doing that work.

The second thing is I have also heard of scams where seniors are being asked to send money urgently because there is some bank account problem, and they are asked to send it at a cryptocurrency ATM. Even the low tech version of fraud is being used to mislead seniors into thinking that that is a way to fix a banking problem.

Mr. Weisman, I lead a bill, the Senior Financial Empowerment Act, which would ensure older adults and their caregivers have access to critical information regarding how to report and combat fraud.

How would consumer education have helped in this situation? Mr. Schildhorn, thank you for sharing your experience. You mentioned that you were asked to wire funds. How can crypto be used as a tool for scammers? What do you believe could be done on the institution and consumer education, and to prevent those type of scams? Both, please.

Mr. SCHILDHORN. Yes, I was a big fan of your bill, particularly the areas of consumer education which are so critical, but the scammers create an emergency and people respond and emotionally.

The thing I found the most interesting was your reference to the ATMs and the cryptocurrency ATMs. They are just the easy access road to sending money to the scammers, and they are unregulated.

As you said earlier, the law is always going to be behind technology, but the kind of regulations you are asking for are eminently reasonable, and these are the kinds of things we have in other areas of the economy. This is what we should be doing.

Mr. WEISMAN. Senator Gillibrand, on an institutional level, I look at the banks because there is one break where the scammer does not have the direct relationship with the victim, and that is at the teller.

Right now, you can't withdraw $9,000 from an ATM. You must have a human interaction with a teller. If banks are required to train their tellers to ask questions when they see an unusual cash withdrawal, that is an institutional change that might prevent scam.

On the individual basis, I think Mr. Romanoff talked about a having a family password, but there is another way to do it as well

by asking a question that only your relative or your child would know for.

For example, if I asked who I thought was my son Brett, what is your brother's middle name? I mean, that would—as soon as you ask that question, there is unlikely to be an answer. To have consumers think of that while their child is hurt in jail is a lot to ask, because it is the emotional part of your brain that is controlling everything you are doing.

The rational part of your brain is suppressed during this, but the teller—the teller possibility is there.

Senator GILLIBRAND. Thank you all for testifying today. This is an urgent crisis in my State of New York, and your leadership and your advocacy is making a difference. Thank you.

The CHAIRMAN. Thank you, Senator Gillibrand. I will turn next to Ranking Member Braun.

Senator BRAUN. Yes, Mr. Chairman, I have one final question. The Medicare Transaction Fraud Prevention Act, which we are rolling out, is to empower CMS to use this tool to catch fraudsters.

I can't believe it currently that they do not, and this is for Dr. Ekin, they do not use beneficiary feedback. This bill would allow that too. What do we lose to actually learn from it when we are not talking to the people that actually get defrauded?

Dr. EKIN. Thank you, Senator Braun, for the question. Actually, one of the major things we are missing is we are not—our algorithms are not adaptive enough because we are not getting the data feedback from the beneficiaries.

If we are able to get that data, even our existing predictive algorithms would be more accurate. Basically, they will—adapt to the real scams in almost more real time fashion. I think that is what we are missing now.

Senator BRAUN. Well, I think—thank you for that answer. I believe getting beneficiary feedback along with being able to use the latest tools—most other places that do well with preventing fraud are already doing both. Thank you.

The CHAIRMAN. Thank you, Ranking Member Braun. I will just have maybe one more question before we wrap up.

I wanted to turn to Mr. Romanoff. You have spoken about how quickly generative AI's use by the public exploded, and it seems we are dealing today with an entirely different landscape than we were even a year ago.

I don't think it would be surprising to anyone here to see even newer technology emerge in the coming year or years that will change it yet again. I wanted to ask you, can you discuss some of the ways you think AI will be used by both scammers and these criminals in the future to prey on customers—I am sorry, consumers.

What should companies be doing now, right now, to protect their consumers and to protect their data?

Mr. ROMANOFF. Yes. I want to start by saying oftentimes the quote around how much time it takes to clone a voice, around three seconds, that data came from 2020. When we think about generative AI and its current hype cycle, this technology has already existed in the wild for many years now.

There is the darknet out there in which there are scammers that are using packaged goods to scam adults, older adults and youngsters as well. That is always going to be an issue. In terms of opportunists, you can address that by watermarking content that is generated by an AI.

The problem with that is that there is always a cat and mouse, or a spy versus spy in terms of identifying that generative AI. What we will see is continued adoption of some of these established scams into kind of the new world of being able to generate content at will, and then probably new scams will emerge over time.

Companies can do a lot by, you know, doing some of the volunteer standards that, you know, the Biden Administration came out with some around watermarking and continuing to do some digital work there to make sure that you can run checks against whether something is generated by an AI versus not.

The other area that I have mentioned in my testimony is multifactor authentication. You know, we are going to need to get better at confirming that, you know, a collar or an image or a voice is actually coming from the originator.

The CHAIRMAN. Thanks very much. I know we are out of time, and I wish we had more time. We have lots more questions. This panel was very informative for us. I am going to go through an opening—or our closing statement.

I did also want to note for the record, Senator Rick Scott was here, was not able to ask a question, but was here for the hearing, and as you might know, Thursdays in the Senate are busy mornings.

Today was a little different because we ended our voting for this work period last night, so a lot of schedules changed. That is why people are in and out and some weren't able to make it, but we are grateful.

The hearing record, of course, will be available to all Senators. I want to start by thanking those who are here today, and especially our witnesses, for providing us information, and by virtue of this hearing, giving this information to people across the country, and hearing in this case, not just from witnesses, but in some cases, people who lived through some of these scams, impacted by highly convincing versions of family emergency scams, including Gary Schildhorn, that we heard from first.

We also heard from Mr. Weismann, who spoke broadly about how scams—broadly about scams themselves and also how he has seen them evolve over his 12 years of operating scamicide and posting a scam of the day, and as you said, Mr. Wiseman, never running out of material, unfortunately.

Mr. Romanoff elaborated more on the rapid growth and evolution of artificial intelligence and how this technology enables scammers to deploy scams quickly and cheaply, and how AI is the perfect tool to deceive even the most skeptical consumer.

Dr. Ekin shared some of his research on fraud in the health care space, and we are grateful for that. It is clear that Federal action is needed. You heard that from some of our colleagues.

The action is needed to put up guardrails to protect consumers from AI, while also empowering those that can use it for good, and yet we need to be cautious of bias in AI. Algorithms, just like hu-

mans, need to be trained not to discriminate. I look forward to moving this conversation forward with my partners in the Senate on this—and on this committee.

To that end, I, along with members of the committee, will be sending a letter to the Federal Trade Commission, FTC, asking that the agency appropriately track AI use in scams in its fraud and scams data base. For those watching this hearing today, I wanted to emphasize that the committee is here as a resource.

Whether you just want to learn more or whether you have been targeted by a scam, or you have questions about a potential scam, you can access our new resources, including the committee's new—newest, I should say, Fraud Book with information, tips, and resources, our brochure on the threat of AI and scams, and a helpful bookmark that with quick tips on online—equipped tips online through the Aging committee's website.

To get to that information, it is aging.senate.gov. If you receive a call, a text, an email, or social media message, and something seems off, and you are skeptical, as we all should be, unfortunately, even more and more skeptical, you can report this to the Aging Committee's fraud hotline.

I will read this number twice. It is 1–855–303–9470. That is 1–855–303–9470. Aging Committee staff are available to answer your calls Monday through Friday 9:00 a.m. to 5:00 p.m., Eastern Standard Time.

You can also watch the video clip that we played at the beginning of the hearing and full clips from all of those individuals impacted on our website. I also want to just note for the record, some—every year we have this Fraud Book, but we don't always highlight the top ten scams. I am just going to read them into the record, so it is clear to people.

These are the top ten scams for the calendar year 2022. Number one, financial services, impersonation and fraud. Number two, health care and health insurance scams. Number three, robocalls and unsolicited calls. Number four, tech scams and computer scams. Number five, romance scams. Number six, Government imposter scams, like the IRS that we noted earlier. Number seven, sweepstakes and lottery scams. Number eight, identity theft. Number nine, business impersonation and shopping scams and Number ten, person in need and grandparent scams that we just heard about. Also note for the record that at the beginning of the—that the beginning of the Fraud Book, starting on pages eight and nine, it is fashioned as an alert. Use of artificial scams—artificial intelligence and scams.

Yve a couple of pages just on the AI threat. That is, of course, new information for so many people, so we appreciate folks reviewing that. I do want to urge all consumers, no matter what their age, young or old, or somewhere in between, to review our website, access our educational resources, watch the full video stories from our participants, which will be longer than the clips.

I also want to note for the record that Ranking Member Braun will be submitting a statement, a closing statement for the record. Again, thank you again to all of our witnesses for contributing both their time and their expertise to this topic.

If any Senators have additional questions for the witnesses or statements to be added to the hearing record, the record will be open until Monday, November 27th. Thank you all for participating today, and this will conclude our hearing.

[Whereupon, at 11:31 a.m., the hearing was adjourned.]

Closing Statement of Senator Mike Braun, Ranking Member

Today, we heard from experts, advocates, and people who have experienced AI scams.

Alongside educating older Americans on common patterns that lead to fraud, it's key that we continue to take a balanced approach.

I hope that we can continue to learn from industry's promising advances and integrate these solutions gradually and carefully.

We can encourage the natural transition of our digital infrastructure and services, rather than be forced to make larger leaps down the line.

The challenge now is largely in identifying where these opportunities lie and applying them safely.

I look forward to working with my colleagues on this, and I thank Chairman Casey for holding this hearing.

APPENDIX

Prepared Witness Statements

Gary Schildhorn
Testimony before the United States Senate Special Committee on Aging
"Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back"
November 16, 2023

Chairman Casey, Ranking Member Braun, and Members of the Senate Special Committee on Aging, thank you for inviting me here today to share my story. My name is Gary Schildhorn. I am an attorney practicing law in Philadelphia, Pennsylvania with over 40 years of experience. I am presenting testimony today because I was the intended victim of a scam that utilized my son's voice. The scam continues to be perpetrated. I will also report on the responses I received from across the country to an article publicizing this event.

In February of 2020, I was driving to my office when my phone rang. It was my son, Brett. He was upset and crying. He told me he needed my help. He said was in a car accident, and he was arrested. He said may have a broken nose and his arm was hurt. The car he hit was purportedly driven by a pregnant woman who was injured. He reported that he was assigned a public defender named Barry Goldstein. He gave me Mr. Goldstein's phone number and asked me to call him right away. I told him I would call Goldstein and call him right back. He said, "you can't, they took my phone, get me out, please."

I am a father and a lawyer. My son was hurt, he was in trouble and a pregnant woman was injured. This call instigated and required immediate action by me.

I first attempted to look up Mr. Goldstein. Before the search results came back, my phone rang. It was Mr. Goldstein. He told me he met with my son. He said Brett was hurt but was going to be okay. He reported that Brett had failed a breathalyzer test at the crash scene. I interrupted him, I said that couldn't be because my son would never drink and drive. He said that Brett told him that but that he drank an energy drink in the morning and that may have caused him to fail the test. He said the Judge had ordered a high bail of $150,000 and that I would need 10% of that amount in cash to bail him out. He said he requested that the judge consider a lower bail. He asked if I was in a position to help my son. I assured him I was. He then gave me my son's case number and told me to call the court and arrange for bail. He provided the number for the court.

I called the number he provided. They answered, "Montgomery County Court House". I explained why I was calling. He asked for the case number, which I provided. He confirmed they were holding my son. He also reported that he was viewing the docket and the judge granted the lawyer's request and had lowered bail to $90,000. He then told me that in order to bail him out I would have to use the county bail bondsman, but that there was a problem. The only bondsman available had a family emergency and was not in town. He advised me that the other option was to post a lawyer's bond with the court. I advised him that I was a lawyer and could post the bond. He responded that I was not the lawyer of record, which means I wasn't the lawyer who entered an appearance on behalf of my son. He also said that by the time the change of lawyer was processed my son would have to remain in jail overnight. He suggested that I call Mr. Goldstein back because he would be able to assist.

I placed the call. Mr. Goldstein agreed to post a bond and informed me I would need to wire him $9,000. He stated he was a member of a credit union, and I would have to go to certain kiosks to wire the money. I later learned that these were bitcoin kiosks. He provided possible locations. He then told me that he was attending an out-of-town conference and would be leaving for the airport in 2 hours. I needed to hurry.

This series of calls all occurred within a few minutes. It was not until the calls stopped and I was driving to the bank that I had an opportunity to think. I called my daughter-in-law, Kim, told her what happened and asked her to alert my son's office that he had been in an accident. I called a lawyer friend in Montgomery County and relayed the story. He said it didn't sound right but he would get right back to me. A few minutes later, I received a facetime call. It was Brett. "Dad, Kim called work and they put me on the phone." "You are being scammed; see, I'm fine."

Shock, relief, and anger—one emotion followed the other. I said to Brett that there was no doubt in my mind that it was his voice on the phone—it was the exact cadence with which he speaks. I sat motionless in my car just trying to process these events. How did they get my son's voice? The only conclusion I can come up with is that they used artificial intelligence, or AI, to clone his voice.

My plan was to keep Mr. Goldstein in the dark while I tried to get law enforcement involved. The Philadelphia police said since I hadn't lost money they would not get involved. The FBI stated that they were aware of this scam but the scammers were using untraceable burner phones and once the bitcoin payment was made it couldn't be recovered. While I was placing these calls, Mr. Goldstein was constantly texting me reminding me that he was leaving for the airport. I was offering excuses for the delay and, at the same time, posing questions to Mr. Goldstein. I advised Mr. Goldstein that I could not find a listing for him in Martindale-Hubbell, a well-known resource for attorney biographies. Mr. Goldstein promptly forwarded me his listing in Martindale-Hubbell, which reflected that he was a well-regarded attorney. I was shocked that he had known what Martindale-Hubbell was and even more so that he had been sophisticated enough to make a fake listing for this scam. When I then asked him for his Social Security Number he cursed me out, told me I didn't love my son and stopped communicating with me.

My anger was replaced by frustration. My law practice had exposed me to securities fraud cases. If I, as a sophisticated lawyer, was almost scammed, there were most certainly people out there losing their money. What was shocking is that there was no remedy for these victims. There was no one to sue or a remedy to retrieve the bitcoin payments, and law enforcement lacked the tools to defeat burner phones and bitcoin transfers. The only available course of action was to publicize this story in the hope people would be forewarned of the scam. I reached out to the Philadelphia Inquirer. They published the story as a front-page article in their Sunday addition. The local Fox news station aired a segment on its morning show.

This scam has not abated. Since the publication of the article, I have received dozens of calls from victims who lost money. They are universally in shock, embarrassed and angry. They all ask what they can do. I recommend two things; they publicize their story and suggest they contact their bank and recommend a policy where bank tellers are required to ask customers why

they may be making an unusual cash withdrawal. Many of the victims told me they were too embarrassed to go public.

This experience has led to the following observations and thoughts: I understand that there are economic benefits to a monetary transfer system, like cryptocurrency, that avoids the regulated bank industry. It is also manifestly apparent that this technology, along with AI technology and burner phones, provide a riskless avenue for fraudsters to prey on us. I doubt that the commercial benefits of cryptocurrency could ever outweigh the economic and social harm it causes. A fundamental foundation of our system is that if you are harmed, a remedy is available through the courts or law enforcement. Unfortunately, that is not the case here.

Written Testimony
Hearing on "Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back"
Senate Special Committee on Aging
Tom Romanoff
Director, Technology Project at the Bipartisan Policy Center
November 16, 2023

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

Thank you for inviting me to testify on this important and evolving topic of AI in Frauds and Scams.

My name is Tom Romanoff, and I am the Director of the Technology Project at the Bipartisan Policy Center. As director, I lead the organization's research and advocacy for bipartisan solutions in the technology sector. Our portfolio includes content moderation, data privacy, digital divide issues, and Artificial Intelligence. The latter is where we kicked off our efforts in technology when, in 2018, we partnered with Representatives William Hurd and Robin Kelly to create a National Strategy for Artificial Intelligence. We helped pass this strategy as House Resolution 1250 alongside seven other bipartisan sponsors. Outside of the Representatives who co-sponsored this work, we also engaged hundreds of experts across civil society, the private sector, and academia.

Prior to my role at the Bipartisan Policy Center, I advised Chief Information Officers and Chief Information Security Officers across the federal government on emerging technologies and compliance with existing regulations. Included in my clients were the Office of Management and Budget, the U.S. Food and Drug Administration, the General Services Administration, and others. In addition to acting as a senior advisor for these officials, I led teams that worked on critical federal-wide initiatives in technology modernization and cybersecurity, including the President's Management Agenda and the Federal Data Strategy.

I commend the leadership of this Special Committee for holding this hearing today, as this is a critical moment for policymakers to consider solutions that will better prepare us for the emerging role of AI in cybercrimes. I want to first level-set on how we got here. As a technology, AI has been around for a while. While its theoretical roots originated in the 50s, since then, data scientists and engineers have discovered increasingly sophisticated ways to leverage the technology to predict and identify data trends.

There are seven main branches of AI, ranging from robotics to natural language processing to deep-learning machines. All these branches of AI are still in the "Artificial Narrow Intelligence" development phase, meaning they can do a given task and are not as smart as a human across different functional areas. However, AI technology is increasingly being leveraged to support daily use that most users may not even recognize – from support with driving your vehicle to unlocking your smartphone.

Over the years, we have seen waves of interest in regulating this technology as new advances demonstrate new capacities. Generative AI, or the ability of a computer to produce content on its own, is the latest in this trend. Without a doubt, Generative AI has a significantly more demonstratable capacity than past AI breakthroughs because of its open (and free) accessibility and availability to most users.

Fast forward to today, Generative AI's capacity has gotten so good that most people cannot tell the difference between computer-generated content and human-generated content. This is due to a couple of factors, the most important of which is a *transformer.* In 2017, transformers were created to allow AI programs to get more done at a faster pace. Since that breakthrough, we have seen advanced capacity across all forms of AI. Robotics, computer vision, deep learning, and Generative AI have all gotten better at their tasks. In the Generative AI space, that means that we have seen advancements in creating, detecting, and accessing synthetic media, commonly referred to as deepfakes (images) or voice cloning. In other areas, it means that AI is also advancing; we do not have access to the output of those advancements freely available.

Generative AI is not inherently bad for our society or precluded from use in scams. In fact, many will argue that Generative AI has many more positive use cases than negative ones. In nearly every aspect of our lives, we can think of a way to deploy Generative AI to increase productivity and improve outcomes. Among aging Americans, for example, it can be used to detect elder abuse, address senior loneliness, and revolutionize medical care. The benefits of this technology have yet to be fully realized, but many in the tech space are working on products to leverage it for positive outcomes.

Despite these and many other benefits, we also know that Generative AI is already being used in cybercrime. Criminals are exploiting this technology to produce manufactured and realistic media. As the good in this technology is explored, we must acknowledge AI's risks and seek a balanced approach, focusing on curtailing abuse while promoting positive uses and innovation.

As a result of its current capacity, Generative AI increases the quality, quantity, and targeting capabilities of fraud-- making it cheaper, faster, and more effective to create idiomatic narratives, deploy multimedia resources, and write malicious code. Combined with opaque legal frameworks and international origins, criminals can now use GAI to coordinate sophisticated attacks with little risk of being caught. Examples include:

- Cybercriminals are leveraging generative AI to augment social engineering campaigns—cybersecurity attacks that use psychology to manipulate people into sharing sensitive information.
- Hyper-realistic voice deepfakes are used to manipulate victims and
- Fake nudes are used to extort in what is called "sextortion."

While many of the victims tend to be younger people, older people are targeted for more in absolute sums. Criminals know they have more money to lose.

Beyond the psychological trauma that comes with these kinds of crimes, the financial losses are skyrocketing. In 2020, Americans lost $3.5 billion to online fraud; by 2022, losses had tripled to nearly $9 billion (Federal Trade Commission). It is important to note that not all these scams have been perpetuated by AI technologies; conflating the total online fraud loss with the rise of GAI is a misrepresentative of the issue. The warning here is that GAI will make it easier and more prevalent as criminals adopt its use in their operations.

Importantly, we are seeing some indications that adoption is coming fast. A 2023 report released by the cybersecurity firm McAfee reported that GAI applications need less than three seconds of a person's recorded voice to produce a convincing clone. In a survey of more than 7,000 individuals worldwide, one in four said that they experienced an AI voice cloning scam. Even more telling is that the survey happened *before* ChatGPT was widely used, showing that voice-cloning technology has been in active use even before popular tools like ChatGPT 3 emerged.

For the elderly community, there are additional obstacles to navigating this new threat. In a survey this year, 68% of Gen X and Baby Boomers said that they do not use AI, with 88% in that demographic unclear about its impact on their lives. That is a problem if potential victims do not know of the technology or its applications.

We know that cyber fraud is a multi-billion-dollar-a-year business. As we navigate the evolving landscape of generative AI, it is imperative to recognize and address the emergent fraud risks associated with generating synthetic data at scale. Here are five risks that pose the greatest danger to older adults:

- Firstly, the creation of deepfakes and the dissemination of misinformation pose significant threats. Generative AI can fabricate highly realistic images, videos, and audio recordings, which can be used to mislead the public, manipulate opinions, and impersonate individuals for malicious purposes.
- Secondly, the rise in sophisticated phishing and social engineering tactics is alarming. AI-enhanced methods can mimic personal communication styles, making fraudulent emails and messages increasingly challenging to distinguish from legitimate correspondence, elevating the risk of individual and organizational data breaches.
- Thirdly, while identity theft has long been a concern, AI makes it much easier and more prevalent. Generative AI can produce authentic-looking images and documents, facilitating the creation of fake identities. This capability can be exploited in financial fraud, the creation of deceptive online personas, and circumventing security measures based on identity verification.

- Fourthly, manipulating financial markets through AI-generated misinformation is a looming threat. Fraudulent actors can use AI to fabricate news or social media content, influencing investor decisions and market trends for personal gain.
- Lastly, the automation of traditional scams, such as romance or lottery scams, has become more efficient and widespread due to generative AI. This amplifies the scale and reach of fraudulent activities, impacting a more significant number of victims and complicating the efforts to combat such schemes.

Solutions

In trying to prevent the use of GAI for crime, many are looking into using the technology to detect and mitigate scams before they result in financial loss. Suppose an AI can detect a Deepfake and label it; that could eliminate a lot of risk for the consumers of that media. It is promising but has some issues- criminals always look for ways to beat the detectors. While publicly available GAI may put a watermark in the digital background, the programs specifically developed to facilitate fraud will not, and they are getting more sophisticated. These could lead to an arms race between deepfake creators and detectors. Our current detectors are unreliable, especially if an adversarial AI is trained to beat it.

This is an area where we have seen a lot of interest from policymakers at both the state and federal levels. Many of the bills introduced in the House are intended to counter the deepfake risk. This is also one of the most popular state-legislature topics, with several states advancing bills to identify and govern synthetic media. Last week, President Biden signed an executive order with sweeping AI provisions, including directing the Commerce Department to:

1) Verify the originality and trace the origins of content.
2) Mark artificially created content, for instance, through watermark methods.
3) Identify artificially generated content.
4) Restrict AI systems from creating content that depicts child sexual abuse.
5) Evaluate tools employed for the tasks mentioned above.
6) Review and manage synthetic content.

Additionally, the Executive Order mandates that NIST provides instructions to federal agencies, particularly concerning the labeling and verification of content they create or disseminate. One of the outstanding questions that needs to be addressed is the definition of synthetic media: does any altered media fall into the category of synthetic media, and how do you distinguish between AI-generated media and replicated media? Another area of consideration is the role that Section 230 has in liability protections for platforms that post these images.

AI does have a role in countering these issues. The only way to process the sheer amount of information and identify patterns across the US criminal network is through a program that can accurately and fairly predict trends. AI will be at the center of that program. Companies who invest in these systems will reap the rewards of lower operational costs and reduced liability. AI can amplify the defense of these systems.

Another way we can address this risk is to adjust and adopt multiple authentication factors in the methods used to validate individuals' identities. For example, some banks now use voice identification to authenticate account ownership. However, criminals have used AI to clone voices to break into a bank's voice banking system. Using multiple authentication processes to validate access and secure assets can address this issue. Biometrics cannot be the only authenticator but can be part of a system of protection.

Further, those creating AI systems must address bias in the data used to train the system, particularly who gets flagged as a potential criminal. For instance, companies have been fined for discrimination in their lending or credit decisions based on zip codes, name suffixes, or other indicators. These are human biases. If those same applications were used to train an AI to predict fraud, the bias and discrimination would be built into a system and scaled up as an organization deploys this program.

In closing, I am leaving you with some reference to which this technology is being adopted and is advancing. In the ten years, this tech has been around, it has gone from computer science theory to widescale use. ChatGPT reportedly hit 100 million users in February after two months of free and public access, an unprecedented technology adoption. Over the last year, AI has been integrated into almost every major tech company's platform, and we have seen many new uses, including in cybercrime, emerge. In the coming months, we will see billions in start-up funding go toward building out this technology's use. Do not let the idea that this is tomorrow's technology cloud the reality of its use today. As I stated in the beginning, we must tackle the abuse while driving toward positive applications to safeguard its adoption.

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.

McCOY COLLEGE OF BUSINESS
TEXAS STATE UNIVERSITY

WRITTEN TESTIMONY OF DR. TAHIR EKIN

submitted to the

UNITED STATE SENATE

SPECIAL COMMITTEE ON AGING

on

Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back

November 16, 2023

Tahir Ekin, Ph.D.

Fields Chair in Business Analytics
Professor of Analytics and Information Systems
Director of Texas State Center for Analytics and Data Science

McCoy College of Business, Texas State University

tahirekin@txstate.edu

McCOY COLLEGE OF BUSINESS
TEXAS STATE UNIVERSITY

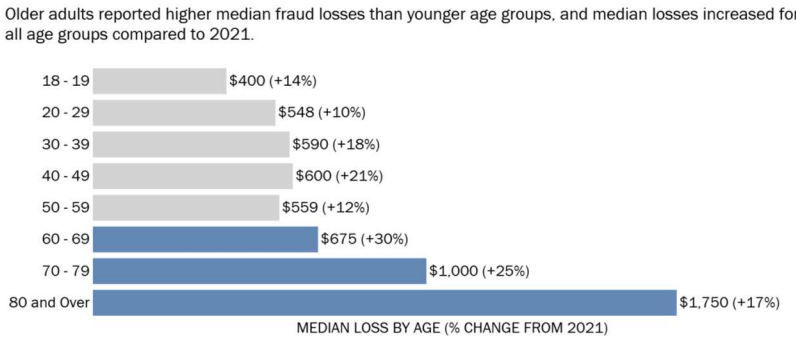
Introduction

Good morning, Chairman Casey, Ranking Member Braun, and esteemed members of the Committee on Aging. Today, as we convene, it is alarming to acknowledge an 81% increase in losses to scams among older Americans, amounting to billions of dollars in the past year[1]. I am Dr. Tahir Ekin, Fields Chair in Business Analytics and a professor at McCoy College of Business, Texas State University. My research delves into the critical intersection of artificial intelligence (AI) and fraud detection. I am honored to testify on the urgent matter of modern scams targeting older Americans and the pivotal role AI plays in both enabling and combatting these threats.

Scams targeting older adults: Role of AI

Scams continue to affect older Americans at alarming rates[2] [3] (refer to Figure 1). Despite improved awareness and educational programs, both the losses and the number of victims have surged[1] (see Figure 2). This prompts the question: Are scammers becoming more sophisticated, or are our responses lagging? The reality likely involves a combination of both factors.

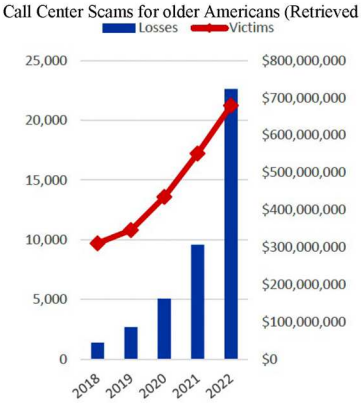
Figure 1. 2022 Median Individual Loss Reported by Age (Retrieved from FTC[3])



Percent change from 2021 shown in parentheses. Median losses calculated based on reports in each age group indicating a monetary loss of $1 to $999,999. Reports provided by IC3 are excluded.

[1] [1] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf. Federal Bureau Investigation. Federal Bureau Investigation's Elder Fraud Report 2022.
[2] https://www.aging.senate.gov/imo/media/doc/aging_committee_fraud_book_20221.pdf. Fighting Fraud: Top Scams in 2022. US Senate on Special Committee on Aging. September 22, 2022
[3] https://www.ftc.gov/system/files/ftc_gov/pdf/p144400olderadultsreportoct2023.pdf Federal Trade Commission. Protecting Older Consumers 2022–2023 A Report of the Federal Trade Commission. October 18, 2023.

Figure 2. Call Center Scams for older Americans (Retrieved from FBI[3])



AI amplifies the impact of scams, enhancing their believability and emotional appeal through personalization. Exploiting individual vulnerabilities, scammers utilize AI to tailor messages, creating almost indistinguishable voice clones with just a brief audio sample. Voice and face manipulation, coupled with emotionally charged content and adaptive responses, elicit urgency or familiarity, manipulating older adults' emotional responses and vulnerability. Notably, there's a surge in personalized scams like the "person in need-grandparent" and romance scams, where AI crafts convincing profiles and identifies emotional triggers through automated conversations.

Recognizing the growing role of AI in scams is crucial. While efforts to halt scammers are underway, a blanket ban on AI might not eliminate adaptive scams entirely. Instead, we should explore AI as a part of the solution.

AI as a solution to stop scammers and protect would-be victims

My research, centered on AI methods for healthcare fraud detection, draws parallels to combatting scams targeting older Americans. Industries, like credit card companies, have successfully used AI for fraud detection, denying suspicious transactions in real-time and collaborating with consumers for confirmation. However, health care fraud still incurs substantial losses as high as 10% of our annual health expenditures, which could mean more than $300 billion[4]. Hence, the name of my book: Statistics and health care fraud: how to save billions[5]. We have limited resources to analyze billions of transactions -Statistics and AI find the needles in the haystack and save taxpayer's money.

[4] https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud. The Challenge of Health Care Fraud. National Health Care Anti-Fraud Association.
[5] Ekin, T. (2019). *Statistics and health care fraud: How to save billions*. CRC Press.

AI's proactive role extends to monitoring online platforms and blocking potential scam attempts, with AI-based call-blocking systems and authenticity verification curbing scam calls. Yet, its true potential lies in collaboration, as seen in government health care programs. Initiatives like the "Medicare Transaction Fraud Prevention Act" advocate data collection and co-verification with beneficiaries, essential for integrating AI successfully, akin to credit card fraud detection. Responsible AI methods can facilitate personalized education campaigns, preserving privacy and ethics. For example, AI can flag atypical behavioral patterns, like sudden financial transactions, enabling tailored alerts and educational materials for older adults. Lastly, fraudsters are adaptive, and scams will evolve. Use of adversarial AI can help proactively limit scammers' abilities[6].

Acknowledging AI's imperfections, such as false positives, and addressing privacy concerns, is crucial. However, by constructing responsible AI systems, we can empower older Americans while navigating potential risks. This necessitates clear objectives and legal checks at the application layer of augmented intelligence.

Policy recommendations and future directions

Addressing the dual role of AI in both perpetrating scams and providing solutions to protect potential victims requires a multi-faceted approach. To effectively combat these evolving threats, collaboration among government agencies, tech companies, financial institutions, and consumer advocacy groups is crucial. Sharing insights and data to train AI models to detect and prevent these scams is pivotal. Including input from older adults in developing AI-driven tools and technologies to proactively detect scams and protect older Americans is also necessary.

In the fight against AI driven scams, awareness and AI literacy are critical weapons. Existing efforts that educate seniors on safe digital practices, such as the work of FTC Federal Advisory Council and the "Pass It On" campaign, can be enhanced to include AI related scams. It is safe to assume that fraudsters play the long game `and can combine doctored videos with stolen identity to build convincing synthetic identities.

There are ongoing efforts to establish oversight bodies or regulatory agencies responsible for monitoring and setting standards for the ethical use of AI. In the context of scams, clear disclosure of the use of AI in communication, marketing, and financial transactions, with a focus on protecting vulnerable populations such as older adults could be important. Knowledge of when one interacts with an AI based system, could help protect older adults.

Accessible support and reporting mechanisms such as toll-free "Fraud Hotline" are crucial against scams. AI based chatbots and communication channels can provide support outside the business hours or at time of need. AI also can make public scam awareness campaigns more impactful making them tailored to the needs of the specific older adults.

Conclusion

The interplay of AI and scams brings forth both challenges and opportunities. Striking a careful balance between fostering AI innovation and protecting vulnerable populations is paramount.

---

6 Ekin, T. (2023) Adversarial Outlier Detection for Health Care Fraud. 2023 AMCIS Proceedings. Panama City, Panama

Advocating for proactive and personalized AI-based supporting measures becomes crucial, recognizing the difficulty in recovering both lost finances and mental well-being after a scam. Prioritizing the enhancement of data and AI literacy among older Americans, and actively involving them in prevention and detection efforts, stands as a cornerstone.

Understanding the impacts of dynamic disruptions like AI will undoubtedly take time. As a realistic optimist, I find hope in ongoing advances, rigorous testing, and evolving regulatory frameworks. The collaborative efforts, I believe, will yield robust and trustworthy AI applications, fostering a safer environment for older adults.

Thank you for providing this platform to address a critical issue. Your work in safeguarding older Americans against scams and raising awareness is commendable. I eagerly welcome any questions or discussions the Committee may have.

Questions for the Record

U.S. Senate Special Committee on Aging
"Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back"
November 16, 2023
Questions for the Record
Mr. Gary Schildhorn

Senator Raphael Warnock

Question:

Congress needs to do more to raise awareness and improve prevention measures against scams that target seniors, especially considering the rise in scams that use artificial intelligence. Scams must be reported and publicized so that we better understand how they work and how they can be prevented in the future.

Mr. Schildhorn, I am sorry to hear about your experience as the intended victim of a scam, and I appreciate you sharing your story. How can we work to reduce the stigma and embarrassment that many scam victims experience so that they will feel empowered to tell their stories?

Earlier this year, I was proud to join my colleagues on the Aging Committee in sending a letter to the Federal Trade Commission (FTC) requesting information about how the agency is tracking and responding to AI scams targeting seniors.

Response:

I have received thousands of responses from people who were scammed and lost money. Perhaps if the media reached out and provided an opportunity to tell their stories, there would be grateful participants. To my great surprise, my testimony has been viewed by over 30 million people. Your committee hearing was the catalyst. It may encourage others to take similar action.

Senator John Fetterman

Question:

Mr. Schildhorn, your chilling story is one of too many in Pennsylvania and across the country. Victims of scams are victims – plain and simple. What would you tell potential victims to help them better identify scams?

Response:

The most helpful suggestion is that each family should have a family password. If the caller doesn't know the password, it's a scam. Another flag occurs when the caller asks that money be sent in an untraceable form such as gift cards or crypto currency. I hope this is helpful.

U.S. Senate Special Committee on Aging
"Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back"
November 16, 2023
Questions for the Record
Mr. Tom Romanoff

Senator Mark Kelly

Question:

The 2022 FBI Elder Fraud report ranks Arizona as fifth in the nation for the number of fraud victims over the age of 60. We rank seventh overall when it comes to the amount of money that those older adults lost. And of course, the numbers are probably higher than those reported here.

While nationwide the number of scams targeting folks over 60 has fallen since its peak in 2020, the dollar amounts of losses have skyrocketed to three times what it was in 2020. In 2022, based on reports from the FTC and the FBI, folks over 60 lost between 1.6 billion and 3 billion dollars.

That's way, way too much money. And this increase comes as we're seeing scammers get more sophisticated with the technology they use. This includes artificial intelligence. But AI can be used for good, too. What are some of the ways AI can help protect seniors or aide law enforcement once a scam has begun—in real time?

Response:

- AI technology has been used for many years to examine data sets in real-time for fraud detection systems, pinpointing atypical behavioral patterns that signal potential fraudulent activities. Banks and e-commerce platforms use machine learning algorithms to identify unusual patterns in transactions, helping them flag potentially fraudulent activities. The massive amount of data needed to detect fraud will only continue to grow, requiring more investments and capacity in AI systems. The countermeasures also need to expand as AI expands the scope of attack vectors (ways in which a hacker gains access or exploits a system).
- AI systems can analyze phone calls and voice interactions, identifying certain speech patterns or keywords associated with common scams. This can be used to alert the potential victim or as a flag for fraud-detection systems to increase their surveillance for suspicious behavior.
- A risk for companies using AI for fraud detection is that they will label an innocent engagement as potentially fraudulent. This is called a "false positive" hit and drives a lot of liability risk aversion. AI can help in this case as well. AI systems can use more inputs to identify fraud than past systems and leverage these inputs much faster than humans.
- Apps on the marketplace are also being used as an additional safety layer. To prevent scam calls, companies are inventing apps that feature "AI-powered assistants" that will answer calls from unknown numbers and filter out unwanted spam and scam calls, only forwarding legitimate inquiries to the user.

Other Examples:

- Using machine-learning techniques based on more than 100 scam calls, artificial intelligence algorithms have been trained to follow the scammer's language and script patterns, with the end goal of disrupting illicit actors' business models and making phone scams economically unviable.
- Researchers from Macquarie University have trained a system that can recognize scam phone calls in real time based on the structure of the conversation, the language employed, and the attempted appeals to emotion used by professional scammers.
- Macquarie University's cyber security hub, Dali Kaafar, and his team have developed conversational artificial intelligence (AI) bots capable of engaging scammers and ultimately reducing the number of people who lose money to global criminals daily.

Question:

Our goal is to protect seniors from deception, fraud, and loss, no matter what method or technology is used. This goal can be accomplished in many ways: We can try to deter or penalize the scammers. We can aim to automatically detect and silence scam calls and text. We can strengthen caller ID and authentication methods. We can focus on citizen education and empowerment. But we may not be able to do everything all at once.

What data sets already exist for training systems to detect and block fraudulent phone calls, emails, and messages? What additional data collection is needed to construct the best defenses in an empirical, data-driven way?

Response:

- Several datasets exist for detecting scams. A literature review published by the Institute of Electrical and Electronics Engineers identified several major popular datasets for training algorithms to detect phishing attempts that can be seen in the table below:

No.	Dataset	Description
1	Phishing Archive	Phishing Archive is an archive of phishing attacks maintained by the APWG. The attacks recorded in this archive were either reported to or detected by APWG [170]. The evaluations of Dhamji et al. [171] and Abburous et al. [172] make extensive use of this dataset.
2	PhishTank	The phishing data reported by the user is stored in the PhishTank website. This information is accessible via API [173] and is shared via a website.
3	Corpora	There were, initially, two components of corpora of the SpamAssassin project: easy ham, as the name suggests, were easily differentiated from spam, and hard ham which were hard to distinguish from spam [174]. There has been a new addition to this corpus in the form of easy ham_2, a ham dataset, spam_3, and a spam dataset [26]. This dataset has been employed by both Fette *et al*. [118] and Khonji *et al*. [175] to evaluate the algorithm PILFER and implement the LUA algorithm, respectively.
4	Enron dataset	Personal emails are included in the Enron dataset [176], which was generated by 150+ employees involved in project CALO [177]. The dataset had integrity difficulties at first, but Bryan Klimt and Yiming Yang [178] were able to repair them. It is regarded as a benchmark dataset, because it contains about 50,000 spam and 43,000 ham emails [26]. The collection of ham messages involves six Enron workers and the TREC 2005 Spam Track public corpus [26]. Georgala *et al*. use the Enron dataset as well for their research [179].

5	TREC	The TREC corpus [180], utilised by Al-Daeef *et al.* is another extensively used dataset [26]. The copyright of this dataset is held by the Waterloo University. The TREC 2005 corpus, which contains 92,189 emails arranged chronologically, and was generated for spam evaluation [26]. There are 39,399 legitimate emails and 52,790 spam emails in the collection. TREC 2006 and 2007 can also be found on their respective websites [26].
6	IronPorts	IronPorts is a defensive mechanism devised by Scott Banister and Scott Weiss in 2000 against Internet threats. In 2007, the Iron Port's corpus [181] was taken by Cisco and has also been employed by Moore *et al.* [182]. A dataset is a collection of data that appear in their spam traps and emails sent to them by consumers. Iron Port's SpamCop [183], created by Jullian Haight in 1998 and acquired by Iron Port in 2003, is a service that keeps track of spam reports from commercial email or UBE recipients (Unsolicited Bulk Emails) with several spam traps in various areas, making it a significant contributor to the Iron Port corpus [26]. SpamCop also analyses all of the reported spam and compiles a list of the systems that were used to send the emails that SpamCop blacklisted [26].
7	Phishload	Phishload is a phishing database produced by Max-Emanuel Maurer in 2012 [184]. Apart from comprising around a thousand legitimate websites, it also contains HTML code, URL, and other data relevant to phishing websites [26].
8	Nazario/Phishing Corpus	The Nazario/Phishing Corpus consists of 7315 emails that were initially collected from 2004 to 2007 and last updated in 2015. The dataset has been used mainly for phishing email detection.
9	SMS Spam Collection	Is used as the public set of the SMS labelled messages, with 5,574 tagged (ham/spam).
10	The Spambase Data set	The UCI data repository of the Spambase Data set has 57 features and 4,601 instances (2,788 emails labelled as spam and 1,813 ham emails) [26]. Mark Hopkins, Erik Reeber, George Forman and Jaap Suermondt from the Hewlett Packard Labs established the dataset [26].
11	Csmining	This dataset includes the emails from six Enron employees extracted from the Enron corpus. One thousand emails were formed and divided into 20% spam and 80% ham. Selection is made from the Enron dataset as it attains a mix of official and personal emails. It does not include the problems present in the rest of the email datasets.

- Companies like McAfee use AI and data for scam detection and presumably use proprietary data.

Senator John Fetterman

Question:

Mr. Romanoff, you highlight that Generative AI is not inherently bad for our society and that it has contributed to advances in fraud detection. How can Congress support these AI innovations to better equip the federal government and private sector in responding to scams and fraud?

Response:

- Identify positive use cases for AI.
- The current trend in policy discussions is to focus on risks and unacceptable uses of AI. But equally as important is identifying the positive use cases. The government is uniquely positioned to demonstrate these positive use cases.
  - Ensure the public doesn't lose trust in the technology by establishing standards and definitions for the types of fraud, including fraud perpetuated by generative AI
  - Biden's EO specifically directs the Commerce Department to establish standards and best practices for detecting AI-generated content and authenticating official content. This helps create a standard to authenticate government communications and materials. This is no small task- there are thousands of registered .gov domains, all of which will need to authenticate materials and communications. The EO also directs the Department of Defense and other agencies to capitalize on AI's potential to improve US cyber defense capabilities.
  - Standardize and define how companies need to respond to incidents,
  - Fund efforts to create clear lines of communication and clarify authorities between federal and local efforts to combat fraud, with a priority on knowledge sharing
  - With fraud prevention spanning the jurisdiction of many agencies, interagency collaboration is critical for presenting a united front in the fight against fraud. Today, the FTC's reportfraud.ftc.gov webpage shares fraud reports with local and state law enforcement partners to help consumers. Expanding on these existing relationships and coordinating efforts like the FBI's Internet Crime Complaint Center would be impactful in protecting Americans against emerging AI fraud threats. Additionally, clearly defined authorities over AI are difficult but needed to ensure these agencies are prepared to meet their assigned jurisdictions. Finally, if these agencies are expected to coordinate, there needs to be resources and staff to do it, along with oversight by Congress to make sure they are meeting mission goals.
  - Ensure that generative AI products are labeled or identifiable through digital watermarking.
  - Sponsor or fund competitions like cyber bug bounty programs that focus on mitigating emerging risks from generative AI
  - Increase AI literacy across the federal government and in state/local jurisdictions through training, hiring, and retention of employees with AI skills.
- AI systems may unintentionally reinforce existing societal biases that perpetuate unequal treatment. The use of biased AI models in cyber fraud detection would have significant consequences. It can also lead to a loss of trust in the systems if they continue to prove ineffective or biased. Unbiased detection models are more likely to accurately identify fraudulent activities across diverse scenarios. Addressing concerns of bias and profiling individuals requires a comprehensive approach, including:
  - Creating consensus standards and definitions around bias and fairness
  - Diversity training data so it is representative and accounts for specific demographics and geographic regions
  - Red teaming and auditing, either self-auditing or by a trusted third-partner, and transparency in AI decision-making processes
  - Diversify the people who see the programs
  - Invest in foundational models that address bias in the training data.
- One area that we can positively point to is the use of generative AI to find patterns across diverse groups. Language barriers are often a challenge in educating on the risks of cybercrime.
Generative AI can be used not only to translate mitigation efforts but also to identify patterns where, in the past, efforts were language-siloed. This can protect against a different kind of bias.
- Increase other efforts that will result in less risk to consumers:

- In addition to AI, better cybersecurity and digital validation are needed as a baseline for all internet users. For example, Multi-factor Authentication as a prerequisite for online transactions could address a significant portion of cybercrime.
- Develop policies that don't hinder the private sector's ability to provide some added layers of security to digital portfolios. For example, there are companies inventing apps that feature "AI-powered assistants" that will answer calls from unknown numbers and filter out unwanted spam and scam calls, only forwarding legitimate inquiries to the user.
- Utilize and reinforce existing regulations around unwanted contacts, such as the "Do Not Call list" and efforts to label and verify callers.

Question:

Mr. Romanoff, there are too many stories of bad actors abusing AI to take advantage of consumers, particularly older Americans. How can we improve technological literacy and awareness of scams among older Americans in addition to supporting positive AI innovations to detect and prevent scams?

Response:

- Recent studies have shown that older adults are enthusiastic about learning and using AIenabled products, but they need more learning avenues. Additionally, they worry that AIenabled products may intrude on their privacy. AI can positively improve the quality of life for seniors, offering personalized experiences, accessibility solutions, increased independence, healthcare treatment, and improved communications and social connectivity. As technology continues to evolve, it is vital to ensure seniors can keep up with the latest advancements and maintain their digital literacy. Technological literacy is crucial for older adults' acceptance and adoption of AI products.
- Older adults may be particularly vulnerable to digital threats, but they typically don't have enough cyber literacy to know the risks and red flags of AI-powered fraud. Educational resources can be offered through beginner-level courses, workshops, and tutorials at employers, community centers, libraries, schools, online resources, or senior care organizations.
- It is essential to increase cybersecurity awareness. Individual negligence significantly contributes to data breaches. Bad security habits include weak passwords, accidentally clicking on phishing links, losing devices, and inadequate employer-led training. Educating older adults on best practices for protecting their data and privacy when using AI-driven tools and services is crucial. By raising awareness and providing guidance on digital security, we can empower seniors to make informed decisions and use AI-driven solutions with confidence.
- Most data breaches involve the human element and often involve social engineering. Social engineering attacks use psychology to manipulate people into sharing sensitive information or granting access to systems. It is less of a cyberattack and more of a confidence game where millions worldwide are deceived and fall victim to scams. Many fraudsters target senior citizens who may need more cybersecurity awareness. Attacks happen frequently enough to merit special consideration and training. In recent years, these attacks have become more targeted, sophisticated, and abundant due to the profusion of online information on individuals of interest.
- Implementing robust data protection measures is vital when developing and deploying AI-driven solutions for seniors. This may include encryption, secure storage, and strict access controls to safeguard users' personal information. Previously, in our AI National Strategy, BPC recommended that federal data privacy legislation is a critical first step toward building trust in AI-specific technologies. If people trust that an AI system will respect their privacy, they will be more comfortable using AI.

U.S. Senate Special Committee on Aging
"Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back"
November 16, 2023
Questions for the Record
Mr. Steve Weisman

Senator Mark Kelly

Question:

In 2022, based on reports from the FTC and the FBI, folks over 60 lost between 1.6 billion and 3 billion dollars. That's obviously a wide range because different databases track different reports. We're relying on people to actively report fraud—and FTC estimates their Sentinel database includes only two percent of losses from people who lost less than one hundred dollars.

That suggests the losses we're actually looking at are closer to 50 billion dollars. What are the obstacles and factors contributing to such low reporting rates, and how can we increase reporting to have an accurate understanding of the full problem?

Response:

There are a number of factors that contribute to what we know is a low reporting rate by scam victims. Primary among these is embarrassment. Many older people are concerned that the elderly are sometimes viewed as not being as knowledgeable as they once were and perceive society as viewing them as lacking the sophistication to recognize when they are being scammed. While there have been studies done at Cornell University and the University of Iowa that indicate that parts of the brain that deal with skepticism become less viable as we age thereby making seniors more susceptible to scams, anyone can be scammed, but seniors may perceive being scammed as just another indication that they are not functioning as well as they may have when they were younger and they are embarrassed by this fact.

Another factor that is somewhat related to the embarrassment suffered by scam victims is that too often seniors may be socially isolated without family or friends they feel comfortable confiding in who might otherwise have convinced the scam victim to report the scam.

In other instances scammers threaten their victims with severe repercussions if they report being scammed leaving the victims too intimidated to take action.

Unfortunately, in some instances the scam victims may not even recognize that they have been scammed. In some investment scams, for instance, they may believe that while they lost their money, the investment itself was legitimate.

In a similar vein, some seniors suffering various levels of cognitive decline may not recognize being scammed by even the most obvious scams.

Finally, the government needs to improve its outreach to the public, particularly the elderly to inform them as to how to report scams and make the process as simple as possible.

As to how we can increase reporting to get a better understanding of the extent of the problem, public education is a critical element in raising awareness of the threat of scams and instructing the public as to how to avoid scams and how to report when they have been scammed.

Such education can and should be done on a macro and micro level. On a macro level, public information campaigns should be done repeatedly using all forms of media, including television, radio, social media and in other platforms frequented on the Internet. Collaborating on scam awareness campaigns with national private companies, particularly those who may provide goods and services to seniors to educate seniors about scams is a win-win for all concerned. In addition, partnering with national organizations such as AARP which does a very good job of raising the public's awareness and understanding of scams would be a positive step.

The late Speaker of the House Tip O'Neill was quoted as saying that "all politics is local" and indeed while scams are a national problem they also dramatically affect people on a local level and trusted local institutions should be enlisted in the battle against scams. Local senior centers as well as other local community organizations should be joined with to present federal government created scam awareness campaigns that would educate the public as to both how to recognize and avoid scams as well as how to report when victimized by a scam.

While national law enforcement such as the FBI does a commendable job in investigating scams and presenting scam related information to the public through press releases and other media, local law enforcement often lack the training or knowledge to better aid in the fight against scams. Federal government created scam education programs should be uniformly provided to local law enforcement both to educate local law enforcement and to make them more knowledgeable and responsive in being able to assist local scam victims as well as present scam education programs to the local citizenry.

I often tell my students at Bentley University that the first answer to almost every question is, "it's about the money." When it comes to scams, the money used to pay the scammers is often wired money, gift cards or cryptocurrencies. Establishing requirements of issuers of banks, gift card issuers and cryptocurrency exchanges to report incidents of scams would be helpful although even more helpful in preventing scams would be for increased efforts to enlist banks, gift card issuers and cryptocurrency exchanges in training to recognize and stop scams before funds are transferred. The Stop Seniors Scams Act championed by Senator Bob Casey is a terrific step in this direction by providing educational materials to retailers, financial institutions, and wire transfer companies to share with their employees.

The mechanisms for reporting scams should be made simpler and accessible through a variety of channels including the present online reporting to the FTC, telephone hotlines, email and mobile apps. The reporting process should also be able to accept anonymous reports from victims who wish to maintain their privacy. The reporting mechanisms should also be available in multiple languages because scams have no language barriers. Along with an emphasis on the greater availability of easy reporting mechanisms should be an emphasis on prompt and continuing responses to victims of scams who can often feel abandoned.

Finally, it is important to constantly update scam information. My blog www.scamicide.com where each day for the last thirteen years I have provided a new Scam of the day illustrates how educating the public about the threats of scams and how to avoid them is a never ending process. Protocols for regular updating of educational materials about scams and how to report them must be implemented to keep up with the scam artists, the only criminals we refer to as artists.

Question:

Our goal is to protect seniors from deception, fraud, and loss, no matter what method or technology is used. This goal can be accomplished in many ways: We can try to deter or penalize the scammers. We can aim to automatically detect and silence scam calls and text. We can strengthen caller ID and

authentication methods. We can focus on citizen education and empowerment. But we may not be able to do everything all at once.

What studies have been done on the best interventions, and what has been proven to be most effective at reducing fraud?

Response:

Studies tend to indicate that educational programs can have a significant effect in reducing the susceptibility of people to scams. One study, entitled "Can Educational Interventions Reduce Susceptibility Financial Fraud" by Jeremy Burke, Christine Kieffer, Gary Mottola and Franscisco Perez-Arce indicated that short educational videos and text had a positive effect on fraud avoidance, but that the effect deteriorated over time, however, continual use of such educational videos and text programs maintained the awareness of people using the educational tools.

Along with educational programs technology measures such as encryption and verification tools to flag robocalls, phishing emails and smishing text messages are also helpful

In addition, there are already a variety of readily available resources that can be used to dramatically protect seniors from scams and identity theft including the following:

a. Credit freezes. In the wake of the Equifax data breach, Congress passed legislation to enable people to freeze and unfreeze their credit reports at no charge. Credit freezes are the best protection against identity theft because even if an identity thief has managed to access a targeted victim's Social Security number, the identity thief would be unable to use that information to get a substantial loan or make a substantial purchase in the name of the targeted victim which would require a review of the targeted victim's credit report. Credit freezes and unfreezes can now be done simply and quickly online at no cost.

b. Credit monitoring. Monitoring one's credit reports to identify indications of identity theft in the early stages is a helpful tool. Prior to the pandemic, federal law allowed people to access a free copy of their credit report from each of the three major credit reporting agencies, Equifax, Experian and TransUnion once a year. During the pandemic the credit reporting agencies allowed people to access their credit reports for free on a weekly basis and just a few weeks ago the credit reporting agencies made the weekly free access permanent.

c. The United States Postal Service has a free service called Informed Delivery by which people can go online and see a photo of the mail that they will be receiving the next day. Being able to see if an important piece of mail is coming is helpful in avoiding mail theft which has increased dramatically in recent years and has led to increased identity theft.

d. The Social Security Administration has a tremendously helpful online service called My Social Security Account which allows you to set up a personal online account with the SSA that enables you to view your earnings history and estimates of benefits as well as manage your benefits online including changing your address or starting or changing direct electronic deposits of your check into a bank account you may designate. This is a very convenient service, but it also provides a great opportunity for scammers who have set up My Social Security Accounts on behalf of seniors who have not already set up such accounts for themselves. The scammers then make changes to the victim's account by directing their benefit checks to be sent to accounts controlled by the scammers so it is important to set one up before a scammer does.

e. Phone security is important and there are numerous services to help screen calls from robocalls and scammers. It is also helpful to sign up for the Federal Do Not Call List. While the Federal Do Not Call List will not prevent a scammer from calling a targeted victim, anyone receiving a call from a scammer offering some kind of phony business or investment opportunity knows immediately that the caller is someone who is breaking the law and not to be trusted.

f. Security software for all of your devices including your phone is very important as is regularly updating your security software with the latest security patches as soon as they are made available.

g. Making sure your router's settings are set to protect you from hacking through Internet of Things devices in your home such as smart televisions or Alexa or Siri.

h. Dual factor authentication should be used for all accounts so that even if your user name and password are compromised, access to your accounts will remain secure.

i. Having a unique password for each of your online accounts is critical. Passwords are often compromised in data breaches. If you use the same password for all of your accounts, your bank account could be in jeopardy because a password you used at another company was compromised in a data breach. And as for data breaches it is not a matter of if you will be affected by a data breach, but when. Password managers are an effective way to have unique passwords for all of your accounts without having to remember them all. If, however, you wish to find that helping hand at the end of your own arm, you could use a strategy of establishing a base password and adapt it for each of your accounts. So for instance, you could use a phrase such as IDon'tLikePasswords as you base password. As passwords go it is pretty strong. Then add a couple of exclamation points at the end of the phrase and you have an even stronger password. You can then adapt it with a few letters for each of your accounts so your Amazon password could be IDon'tLikePasswords!!AMA.

j. Security questions which allow you access to your account or enable you to change your password if you forget your password are an important part of your security. However, cybercriminals have been able to gain access to people's accounts by answering the security question, the answer to which may often be found by a determined hacker on the Internet or even in your own social media. There is a simple solution however and that is to give a nonsensical answer to the security question. There is no rule that requires you to answer the security question honestly. So if your security question is what is your mother's name, you could make the answer "firetruck" or something else similarly ridiculous. It is so ridiculous, you will remember it and no hacker will ever be able to guess it.

Question:

You have catalogued and reported on many different kinds of scams, from phone calls to phishing emails to fake dating profiles. What data sets already exist for training systems to detect and block fraudulent phone calls, emails, and messages? What additional data collection is needed to construct the best defenses in an empirical, data-driven way?

Response:

Both Android phones and iPhones come with built in spam blocking tools, however there are a number of specialized apps that you can purchase that will do a better job of blocking spam and scam calls as well as use AI to screen unknown calls and text messages and automatically block those deemed to be spam or scams. There also are a number of good apps that will block robocalls.

In addition, many security software programs can recognize both phishing emails and malicious websites. Also most browsers such as Google Chrome, Mozilla Firefox and Microsoft Edge have incorporated security features to recognize malicious websites.

Artificial Intelligence is a double-edged sword and while much emphasis has been made as to how it is being used by scammers, it is also being used along with Machine Learning to dramatically improve the quality of the technical tools used to recognize and block many scams. Even more improvement in this area is needed, but it is very promising.

Senator Raphael Warnock

Question:

Congress needs to do more to raise awareness and improve prevention measures against scams that target seniors, especially considering the rise in scams that use artificial intelligence. Scams must be reported and publicized so that we better understand how they work and how they can be prevented in the future.

Mr. Weisman, how can Congress leverage the FTC's existing authority over consumer protection to improve detection and prevention of AI scams?

Response:

It is clear under the FTC's broad authority pursuant to the FTC Act that it has the authority to enforce existing regulations as well as create new regulations specifically related to AI use in scams. The FTC has the authority to take legal action against anyone or any company using AI in a deceptive manner harming consumers. In addition, the FTC can play a significant role in educating the public about AI scams.

The FTC also can play a significant role in collaborating with tech companies in regard to developing strategies to reduce the use of AI in scams.

One creative tactic used by the FTC already is their Voice Cloning Challenge to promote the development of new strategies to protect people from AI voice cloning technology that is already being used by scammers in scams such as the Grandparent or Family Emergency Scam where the targeted victim receives a call in the middle of the night apparently from a family member who has an emergency and is in need of money to be sent immediately. This scam which has been perpetrated for years has become much more convincing due to the scammers ability to obtain a mere thirty seconds of audio from sources such as social media of the person they are impersonating and use it to clone that person's voice and make the plea of the scammer even more convincing.

Between January 2nd and January 12th the FTC is accepting submissions with strategies for preventing voice cloning by unauthorized users as well as ways to detect cloned voices. The winner of the challenge will receive $25,000 from the FTC. This is actually the fifth time that the FTC has used this type of challenge with a cash prize to address similar problems. In 2012, the challenge was to find a way to defend against robocalls and in 2017 the challenge related to security vulnerabilities found in the Internet of Things.

Finally, the FTC can collect data related to scams involving AI to better understand the problem.

Congress can work with the FTC and armed with data collected by the FTC help pinpoint the problems posed by AI scams and develop legislative solutions.

Statements for the Record

Statement of Hoda Heidari[1], Ph.D.
K&L Gates Career Development Assistant Professor in Ethics and Computational Technologies at Carnegie Mellon University

Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back

United States Senate Special Committee on Aging

Nov 27, 2023

Chairman Casey:

AI technologies are rapidly gaining prevalence and potency, exerting a profound influence on the daily lives of the American people. Their impact spans finances and economic activities, access to healthcare services, and a variety of social benefits. While AI holds the promise of fostering economic growth, improved productivity, and efficiency, it can pose heightened threats to human rights and well-being. These risks encompass adverse effects on agency and self-determination, economic freedom, privacy, the right to humane treatment, and access to justice. To make matters worse, the risks and benefits of AI are not evenly distributed. The vulnerable segments of society are disproportionately susceptible to harm, while the privileged are more likely to reap the benefits. Older adults, in particular, face an elevated risk of harm from the widespread availability and potency of advanced generative AI models. Therefore, safeguarding their interests requires urgent attention to matters of *accountability* and *governance* of AI, addressing the development, release, and utilization of the technology, with a focus on fortifying benefits and mitigating risks.

Aging Adults Are at an Increased Risk of AI-powered Scams.

The most recent wave of powerful AI technologies, referred to as Generative AI, allows their users to produce hyper-realistic images, voices, and videos **cheaply**, **quickly**, and **at scale** without the need for special equipment, skills, or expertise, substantially **lowering the barrier** to committing intricate, large-scale fraudulent schemes. Using small amounts of data,

[1] I am the K&L Gates Career Development Assistant Professor in Ethics and Computational Technologies at Carnegie Mellon University (CMU), with joint appointments in Machine Learning and Societal Computing departments in the School of Computer Science. I am also affiliated with the Human-Computer Interaction Institute and Heinz College of Information Systems and Public Policy. My research is broadly concerned with issues of fairness and accountability when Artificial Intelligence and Machine Learning are utilized to facilitate decision-making in socially consequential domains. My work aims to create and evaluate measures, processes and guidelines for the responsible and ethical use of the technology. I co-founded and co-lead the university-wide Responsible AI Initiative at CMU, and I am a faculty leader at the Block Center for Technology and Society.

Generative AI models can **personalize and adapt** their output to a specific audience—e.g., by imitating the writing style, the voice, or the picture of a loved one in distress. Using Language Learning Models (LLMs), scammers can interact with large numbers of victims simultaneously to build relationships over time and ultimately exploit the emotional vulnerabilities of their targets for fraudulent gain. The ability to clone the voice of a friend or family member can make these interactions believable and difficult to distinguish from conversations with a real human being.

These challenges are aggravated in older adults who are often experiencing initial decline in cognitive functioning. Older adults also experience increased need for care and social connection and they are less likely to be familiar with the capabilities of emerging technologies, such as Generative AI. Therefore, older adults face an elevated susceptibility to fraud perpetrated through AI technologies, perpetuating structural ageism.[2]

(Generative) AI Is Not New. Why Should We Take Action Today?

While Generative AI has existed for several decades, their capabilities have notably advanced in the last two years, thanks to **readily available data** (e.g., the data that can be extracted from the web and other publicly available sources), inexpensive labor to process the data (e.g., annotation through crowdsourcing platforms), and breakthroughs in **hardware engineering** (both compute and memory). Today, massive statistical models (e.g., deep neural networks) can be fit to large swaths of data, giving rise to the so-called *foundation models*–general-purpose AI models capable of performing high-level tasks, such as generating text or images.

Foundation models have substantially altered the dominant paradigm of developing and using AI models. Instead of creating statistical models from scratch, foundation models serve as a starting point from which domain-specific models can be fine-tuned and built without the need for large-scale domain-specific data or prohibitive computing resources. Several powerful foundation models (e.g., LLaMA or Stable Diffusion) have been fully released to the public[3], in some instances, **without adequate guardrails and evaluations**. Due to the **widespread accessibility**[4] of these general-purpose, unrestrained models, the landscape of risks and harms has undergone sudden, significant changes in a wide range of domains.[5]

---

[2] The team "ageism" describes the stereotyping of and discrimination against older adults. While ageism can result in discriminatory behavior, a growing body of research also shows that it can also affect one's physical and cognitive health and well-being and even reduce one's life span. See, e.g., Breaking the Age Code: How Your Age Beliefs Predict How Long and Well You Live. by B. R. Levy, 2022. HarperCollins.

[3] See The Gradient of Generative AI Release: Methods and Considerations by I. Solaiman, and Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI by D. G. Widder, S. West, and M. Whittaker.

[4] Notably, ChatGPT gained more than one million users in less than one week after launch. The same milestone took several years for older social networking platforms. See ChatGPT sets record for fastest-growing user base - analyst note.

[5] See EPIC's report on "Generating Harms: Generative AI's Impact & Paths Forward", 2023.

Recommendations to Protect Aging Adults Against AI-Fueled Scams

1. Raising awareness of AI capabilities is our first line of defense.

Accessible, engaging educational material targeting at-risk[6] and aging populations is likely the most effective avenue for preventing frauds fueled by Generative AI. This will require input and participation by aging adults, to identify the appropriate medium[7] and level of detail.

Such educational campaigns should include the following components:

- **Concrete examples** illustrating the capabilities of modern Generative AI and the ease at which fraudsters can utilize them—e.g., with simple text prompts, one can create fictional images or videos involving well-known individuals.
- **Strategies to verify** the source and veracity of the content using both technological (e.g., installing software/apps designed to detect AI-generated content) and non-technological tools (setting verbal passcodes with loved ones; asking them to respond to security questions; following tips to identify AI-generated content[8]).
- Basic **cybersecurity hygiene** tips include not sharing personal data online and limiting connections to friends and family on social networking platforms. (Aside from protecting sensitive data such as address, date of birth, and social security numbers, it is important for older adults to know that *as little as three seconds* of someone's voice recording is sufficient to clone their voice.[9])

Creating, maintaining, and publicizing a **repository of AI-powered scams** can be another effective tool to instill healthy skepticism in consumers and make it harder for scammers to develop novel, convincing fraudulent schemes. The repository can also serve as a benchmark for AI developers aiming to create technical remedies to counteract deceptive uses of AI.

2. Technological remedies will be useful but inadequate in isolation.

Institutions handling financial transactions, text messaging and phone conversations must strengthen their **central mechanisms to detect and slow down AI-powered fraudulent activities** (e.g., by requiring multi-step verification and justification for withdrawing large sums of money, or automatically detecting and warning the receiver of AI-generated scam).

2.1. Watermarking—promise and shortcomings:

---

[6] See, e.g., Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions by Sheng et al. (2010) for an analysis of at-risk populations for Phishing.

[7] For example, we need to first understand the common sources of information consumed by older adults—TV, traditional or social media.

[8] See, for instance, the Better Business Bureau's guide on detecting fake images, videos or AI-generated text.

[9] Beware the Artificial Impostor. A McAfee Cybersecurity Artificial Intelligence Report. 2023.

Major tech companies, such as Google, Amazon, OpenAI, and Microsoft, have voluntarily pledged to develop technical mechanisms (such as *watermarking*) to inform users of when content is generated by their AI models.

While watermarking is an essential tool that should be required as part of a multi-layer solution, it is not adequate on its own. First, foundation models with no provenance mechanisms embedded in them have already been released publicly, and it will be virtually impossible to recall them. Second, malicious actors will attempt to get around watermarks and other built-in guardrails[10], and staying one step ahead of them will be a perpetual challenge. Cryptographic watermarks are harder to remove, but only apply to voice, image, and video data–not to text-based interactions. Invisible (e.g., cryptographic) watermarks are only effective if consumers know about their existence and have the tools and resources (e.g., software and apps) to put them to use.

2.2. Fraud detection algorithms—promise and shortcomings:

Another technological remedy to the rising level of AI-abetted fraud is through *fraud-detection algorithms*. These algorithms rely on mining patterns in datasets of financial transactions—containing both legitimate and fraudulent activities. These patterns can be utilized to flag irregular activities and warn consumers or financial institutions of potential fraud.

While fraud detection algorithms are attractive solutions due to their *scalability* and relatively *low cost*, they require access to massive, high-quality training datasets and careful engineering. Otherwise, various **biases in data and design choices** can hinder their efficacy. In practice, AI-fueled fraud is likely to be *under-reported*, reporting is in *a non-standardized format*, and the reported data can quickly become *outdated*. If fraud-detection models are tuned improperly, they can falsely flag legitimate transactions as potentially suspicious, limiting the agency and independence of older adults in the process. Finally, these algorithms may cause additional privacy and security risks if they rely on training data consisting of sensitive personal data.

3. Support AI governance and accountability efforts.

As the number of AI-related harms continues to rise, momentum for improving AI governance and accountability is at an all-time high. The public interest requires a strong governance ecosystem to reinforce benefits and minimize risks. Fortunately, comprehensive legislation to implement safeguards around AI has gained strong bipartisan support.

3.1. Regulate the release of and access to foundation models.

Fraudsters often rely on readily available AI models to fuel their schemes. It is, therefore, urgent to mandate guardrails surrounding how foundation models are released and accessed.

---

[10] Universal and Transferable Adversarial Attacks on Aligned Language Models. A. Zou, Z. Wang, J. Z. Kolter, M. Fredrikson, 2023.

While open-sourcing these models democratizes research, innovation, and economic growth, and fosters transparency, it simultaneously supercharges fraud. Potential remedies include r**equiring provenance mechanisms** (such as watermarking) and **stress testing of these guardrails** prior to the release of foundation models.

3.2. Pay close attention to enforcement mechanisms.

A major challenge surrounding AI accountability is enforcement: identifying and holding wrongdoers accountable proportionate to their role in facilitating the harm in question.[11] Using gen AI to defraud aging adults subjects them to cruel, inhuman, or degrading treatment, and it arbitrarily interferes with their lives and well-being. As such, it can be recognized as violating their human rights. Given the recent surge in the corresponding risk levels, providing justice through legal channels is an urgent matter of policy debate. Effective enforcement requires recognizing the vast network of actors contributing to the development, deployment, and use of powerful AI models[12], and allocating liability proportionately and with **deterrence and recourse** as explicit objectives.

[11] In a policy brief by the Responsible AI initiative at CMU, we outline the unique challenges of fostering AI accountability and make several recommendations for addressing them.
[12] Toward Operationalizing Pipeline-aware ML Fairness: A Research Agenda for Developing Practical Guidelines and Tools. E. Black, R. Naidu, R. Ghani, K. T. Rodolfa, D. E. Ho, and H. Heidari, 2023.

Written Testimony Submitted to the United States Senate Special Committee on Aging
Provided for the Hearing:
"Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back"
November 2023

Dr. Shomir Wilson, Assistant Professor and Director of the Human Language Technologies Lab
College of Information Sciences and Technology, Pennsylvania State University
https://shomir.net - shomir@psu.edu

Introduction

First, I wish to thank Chairman Casey, Ranking Member Braun, and the rest of the Special Committee on Aging for the opportunity to provide this written testimony. I also thank the policy aides I spoke with prior to submitting this testimony for identifying my work and contacting me to make this testimony possible. Outreach of this kind is an important part of my work as a professor, and I am glad to contribute to the public record.

I am an Assistant Professor of Information Sciences and Technology at the Pennsylvania State University, in University Park, PA. I direct the Human Language Technologies Lab, which conducts research in natural language processing (NLP), privacy, security, and computational social science. NLP is the branch of artificial intelligence (AI) that focuses on extracting meaning and structure from natural languages (i.e., those languages that people write and speak, which are different from the languages we use in mathematics or to write computer programs). I received my Ph.D. in Computer Science from the University of Maryland in 2011. This testimony reflects my own views and not necessarily those of my present or past affiliations.

My lab's research covers several themes, and one of them is studying variations in scam emails, i.e., the diversity and nuances in malicious emails intended to deceive the recipient for the sender's financial gain. These include attempts to steal sensitive information like passwords or bank account numbers, blackmail threats, illicit employment opportunities, illegitimate financial schemes, ads for fraudulent online retailers, and numerous other security threats [1]. In this testimony I describe our work to characterize the kinds of scams sent to university email addresses [2, 3] and to identify variations between collections of scam emails written in different natural languages [4]. Following that, based upon background knowledge of NLP and security, I describe some likely ways that scammers are using (or soon will use) NLP to enhance their operations.

Email Scams Targeting University Email Addresses

My lab recently published a paper on topics and trends over time in scam emails sent to university email addresses [2]. Some universities' information technology (IT) departments post to the web examples of email scams received by their employees or students, and we gathered a collection of 5,155 of those examples from the websites of five large US universities. Universities' IT departments post these examples to provide scam awareness and education for their respective email users, and gathering them into a *corpus* (i.e., a collection of text) enables us to use data-driven methods to study scams. We note the results could contain representation biases, as IT departments may selectively post the scams that they deem the most pernicious or the most likely to deceive email users. For the present context, we made no assumptions about whether these scam emails were AI-written or human-written.

We used machine learning methods to automatically sort the full set of emails into subsets that were similar to each other, and nearly all of those subsets represented cohesive

topics. Below is a list of topics and examples for each subset (except one, *Miscellaneous*, a placeholder for a subset that lacked a clear theme). Some of them confirm observations from a prior study by our group that focused solely on scam emails sent to Penn State addresses [3].

- *Email Account-Related* (claims that the recipient's mailbox is full or that a message awaits them on the server)
- *Personal Requests* (requests from a colleague or supervisor, for example, to buy a gift card as a token of appreciation for a potential donor to the university)
- *Document Links* (hyperlinks claimed to be to online documents that, instead, lead to malicious websites)
- *Password* (requests for the user to update their password for a university system, instead leading to their password being stolen by a scammer)
- *Employment Opportunities* (job solicitations or offers for the recipient, who is typically a student)
- *Order or Payment* (notifying the recipient that they need to make a payment or a payment has been made on their behalf)
- *Students With Disabilities* (someone, typically claiming to be a university employee, advertising employment opportunities for students with disabilities)
- *Blackmail* (claiming to hold harmful information about the recipient, with a demand for a payment to prevent public disclosure of the information)
- *Miscellaneous* (not a theme; this subset lacked thematic cohesion)

The corpus contained scam emails from mid-2014 through 2022, and we observed certain topics ebbing and flowing over time. For example, *Document Links* and *Email Account-Related* scams peaked between 2016 and 2017, while *Employment* and *Order or Payment* scams have increased in popularity over the past three years.

The selection of topics and the existence of trends over time suggest that scammers perform some tailoring to email users' wants or anxieties. In particular, the *Employment Opportunity* and *Students With Disabilities* themes are acutely relevant to college students' concerns. Scammers appear to be motivated to create scams for the university audience, which suggests that they create scams for other specific groups as well.

Email Scam Variation Across Natural Languages

Our group also published a comparative study of email scams in different natural languages [3]. Using Anti-Fraud International[1], a popular anti-scam web forum, we collected scam emails that were written in three languages: English, French, and Russian. Similar to our study of the university scams corpus, the results may contain representation biases, as users of this web forum may not represent the population at large and they may post only the email

[1] https://antifraudintl.org/

scams that they deem the most pernicious or the most likely to deceive email users. Again, we make no assumption about whether these scams are AI-generated.

We performed a keyword analysis of sets of scams in English, French, and Russian and found similarities and differences in the topics of scams in each respective language. For example, although scams that led with a financial incentive were common across all three languages, scams that led with romantic overtures were more frequent for French and Russian than for English. Within financial incentive scams, purported lotteries were disproportionately popular in Russian, and purported offers of government assistance were disproportionately popular in English.

These variations have several possible explanations. Some explanations come from the biases in the web forum as a sample of scam emails: we cannot determine how representative they are of scam emails at large. (This is actually an obstacle for research on scams in general: privacy concerns, which are reasonable and appropriate, prevent researchers from directly collecting large volumes of scam emails from people's email accounts and phone records.) Other explanations involve cultural differences between the respective populations of English, French, and Russian speakers. Scammers could be actively tailoring the scams for their audiences, or unknowingly they could be reflecting underlying cultural norms.

Likely Implications for Artificial Intelligence in Scams

Scams are perpetrated in natural language, either written (often emails or text messages) or spoken (phone calls). NLP is likely to play a growing role in scammers' activities, as it enables them to reach large audiences with sophisticated forms of deception. In a way, this is part of a continuing trend of technology enabling scammers to reach progressively larger audiences: for example, widespread adoption of email made contacting thousands of potential victims much cheaper than contacting them via postal mail. However, recent NLP systems like ChatGPT[2] can be potent tools for scammers seeking to automate their operations.

One way that scammers can use NLP is to *customize lead-ins to potential victims*. My lab's research showed signs that scammers are attentive to the expectations and anxieties of groups of potential victims, but writing a more personalized lead-in—for example, using publicly available information about an individual's interests and personal history—is time-consuming for a scammer. *Spearphishing* (customizing a scam for a specific person [5]) is a known activity, but until recently the scammer's time and effort limited how many people they could spearphish. AI can enable a scammer to customize a large number of lead-ins, limited only by computational resources that are relatively cheap to purchase.

Another way scammers can use NLP is *to scale up human-like interactions* via written or spoken language. Some scams involve a period of trust-building, where the scammer builds

[2] https://chat.openai.com/

rapport with the victim prior to asking for sensitive information. Building rapport is time-consuming and requires the kind of conversational attention that, again until recently, required significant human time and effort. However, automating conversations with potential victims while guiding them toward exploitation is now within reach of conversational AI systems. With technical skill and cloud computing resources, a scammer could (for example) initiate a large number of phone calls or email conversations at once, each between a conversational AI system and a potential victim.

Note that my lab has not studied AI-enabled scams specifically, and I cannot state with certainty that the above strategies are being used. In fact, it is likely that scammers who merely use speech synthesis (i.e., using a computer to generate an artificial voice that transforms text into speech) to disguise their voices are sometimes being mistaken for more sophisticated AI. However, the financial incentives of using AI are too great to expect scammers to ignore them. Data-driven research on how scams are changing, performed by academia and industry, will help us understand how to counteract these growing threats.

Acknowledgements

I owe thanks to the graduate and undergraduate students in my lab who make our research possible. It is common in computing disciplines for research advisees to perform significant intellectual and technical tasks toward research goals. These students are my collaborators, and I am glad to work with them.

Research featured in this testimony was supported in part by Penn State's Center for Security Research and Education and by the NASA Pennsylvania Space Grant Consortium Research Internship Program.

References

[1] M. Jakobsson, Ed., *Understanding Social Engineering Based Scams*. New York: Springer, 2016.

[2] G. Ciambrone and S. Wilson, "Creation and Analysis of a Corpus of Scam Emails Targeting Universities", in *Companion Proceedings of the ACM Web Conference*, 2023.

[3] D. Pan, E. Poplavska, N. O'Toole, S. Wilson, "Comparing Scam Emails and Email User Education at Universities", in *The Eighteenth Symposium on Usable Privacy and Security (poster abstracts)*, 2021.

[4] D. Pan, E. Poplavska, Y. Yu, S. Strauss, and S. Wilson, "A Multilingual Comparison of Email Scams", in *The Seventeenth Symposium on Usable Privacy and Security (poster abstracts)*, 2020.

[5] B. Parmar, "Protecting against spear-phishing", in *Computer Fraud & Security* 1, 2012.

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

November 16, 2023

The Honorable Bob Casey
Chairman
Special Committee on Aging
United States Senate
G16 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Casey:

Thank you for holding a hearing in the U.S. Senate Special Committee on Aging entitled "Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back."

SSA annually delivers over $1 trillion in Social Security benefits to Americans. This makes SSA funds – particularly the delivery of those funds by electronic means – susceptible to fraud facilitated by Artificial Intelligence (AI). As the Inspector General for the Social Security Administration (SSA), I am similarly concerned about how fraudsters will utilize AI to increase the frequency and sophistication of scams against older Americans.

The SSA Office of the Inspector General (OIG) is a key federal player in the fight against government imposter scams. Our goal is also to be at the forefront of AI-related issues by committing to learning to leverage AI using advanced algorithms to spot abnormalities and outliers to detect fraud, improve decision making, and develop an understanding of how AI can be used to commit malicious behavior.

Disrupting Social Security-Related Government Imposter Scams

Government imposter scams remain a major issue and an opportunity for fraudsters to prey upon the American public. SSA OIG has taken a multi-disciplinary approach to combatting Social Security-related government imposter scams. While SSA OIG has seen a precipitous decline in the number of SSA-related imposter scam allegations from 2020 to the present, according to data from the Federal Trade Commission (FTC), Social Security-related scams remain the top-reported government imposter scam as of November 2023. Therefore, we continue to focus on disrupting these scams.

Shortly after my confirmation, in October 2019, I established a Major Case Unit (MCU). The MCU was created to better handle emerging major fraud schemes against SSA programs and operations, including government imposter scams. Investigating large-

scale organized fraud often requires a multi-disciplinary effort with enhanced legal and analytical capabilities, and coordination with multiple law enforcement agencies around the country. MCU was specifically organized and staffed to conduct multi-jurisdictional investigations of this complex nature. In particular, the MCU works zealously to develop leads, prosecute criminals, and disrupt the scams. For example, our work with federal and state partners have led to the prosecution and sentencing of multiple individuals involved in telephone imposter scams originating from overseas call centers.

Our attorneys also notify domestic gateway providers (who serve as intermediaries between foreign providers and downstream U.S. carriers and pass through millions of calls daily) of their potential civil liability under a consumer protection law within the Social Security Act. In doing so, our team of attorneys educate these domestic gateway providers on the applicability of this statutory provision, encourages proactive techniques to block transmission of scam calls, and, where appropriate impose fines. Further, SSA OIG collaborates with all levels of government, leverages anti-fraud interests of private companies, and engages with special interest groups who focus on combatting fraud and protecting and reaching vulnerable populations. SSA OIG regularly engages with the news media to broaden consumer education efforts, including through television, radio, print, social media, and podcast interviews.

SSA OIG collaborates with SSA to hold an annual Slam the Scam Day during National Consumer Protection Week. Slam that Scam Day educates the public about the tactics scammers use and encourage the public to hang up on scammers. The fourth annual Slam the Scam Day in 2023 garnered an approximate audience of over 86 million people, including television, radio, online, and print audiences. In 2023, Senator Susan Collins was the sponsor of S. Res. 101. With your, Ranking Member Mike Braun, and members of the Special Committee on Aging, Senator Raphael Warnock and Senator Mark Kelly's cosponsorship of this resolution, it passed with unanimous consent.

Addressing Artificial Intelligence

Artificial intelligence is rapidly becoming a primary driver of emerging technologies and is impacting society in ways the public and private sectors are just beginning to understand. According to the National Institutes of Justice, AI is becoming an important technology in fraud detection. Internet companies and financial institutions thwart fraud attempts by using large data sets to continuously train their fraud detection algorithms to predict and recognize anomalous patterns indicative of fraud. AI will be a powerful tool to support the federal government's ability to detect and prevent the fraudulent disbursement of taxpayers' dollars. However, AI will also be a powerful tool for criminals to commit fraud. Criminals will use AI to make fraud schemes easier and faster to execute, the deceptions more credible and realistic, and ultimately, the fraud more profitable.

SSA OIG is in the early days of understanding how criminals will leverage AI to commit fraud against SSA, but we have some understanding based on recent experience. In 2020, SSA OIG agents initiated an investigation into widespread SSA direct deposit

benefit diversion. Agents discovered a "chatbot"[1] was used to impersonate beneficiaries, contact SSA customer service representatives, change SSA beneficiaries' direct deposit account information, and divert their monthly benefit payments to spurious accounts. Like the impersonation scams OIG investigates, the chatbot numbers originated from overseas. The chatbots were effective in moving stolen Social Security benefits into the stream of criminal commerce here in the United States, where organized rings of "money mules" collected and moved the proceeds. We believe this is just the beginning of the potential harm AI can cause to the delivery of Government benefits to the American public.

I recently established an OIG internal Task Force to study AI and related technology. From this effort, SSA OIG expects to determine the tools, processes, and staffing we need to detect, investigate, and deter AI-related fraud and to leverage AI in these efforts. SSA OIG will continue to work with longtime federal law enforcement partners to stay current in the detection, investigation, and deterrence of AI-related fraud. SSA OIG will engage with agencies like the FTC and Federal Communications Commission, who have proven capable partners in our fight against imposter and telecom fraud. SSA OIG will also collaborate with SSA to understand how the agency plans to use AI in its operations, and will review any applicable risk assessments, vulnerabilities, and/or efficiencies gained utilizing AI in SSA programs. Additionally, with our oversight tools, we plan to assist SSA to address AI threats to the agency and to Social Security beneficiaries.

I trust this information is helpful and if you should have any follow-up questions or concerns, please feel free to send them to OIG's Congressional Affairs Advisor Jonathan Blyth at Jonathan.J.Blyth@ssa.gov.

Sincerely,

Gail S. Ennis

Gail S. Ennis
Inspector General

[1] A computer program designed to simulate conversation with human users, especially over the Internet.

○