

**FIGHTING FRAUD:
HOW SCAMMERS ARE STEALING
FROM OLDER ADULTS**

HEARING
BEFORE THE
SPECIAL COMMITTEE ON AGING
UNITED STATES SENATE
ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

WASHINGTON, DC

SEPTEMBER 19, 2024

Serial No. 118-23

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

WASHINGTON : 2025

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

	Page
Opening Statement of Senator Robert P. Casey, Jr., Chairman	1
Opening Statement of Senator Mike Braun, Ranking Member	2
PANEL OF WITNESSES	
Kathy Stokes, Director, Fraud Prevention Programs, AARP Fraud Watch Network, Washington, D.C.	4
Scott Pirrello, Deputy District Attorney, Head of Elder Abuse Prosecutions, San Diego District Attorney's Office, San Diego, California	6
Susan Whittaker, Administrative Assistant, Lehigh County Aging and Adult Services, Allentown, Pennsylvania	7
Nancy Gilmer Moore, Program Director, Indiana Senior Medicare Patrol, Indiana Association of Area Agencies on Aging, Indianapolis, Indiana	9
CLOSING STATEMENT	
Closing Statement of Senator Mike Braun, Ranking Member	29
APPENDIX	
PREPARED WITNESS STATEMENTS	
Kathy Stokes, Director, Fraud Prevention Programs, AARP Fraud Watch Network, Washington, D.C.	34
Scott Pirrello, Deputy District Attorney, Head of Elder Abuse Prosecutions, San Diego District Attorney's Office, San Diego, California	39
Susan Whittaker, Administrative Assistant, Lehigh County Aging and Adult Services, Allentown, Pennsylvania	42
Nancy Gilmer Moore, Program Director, Indiana Senior Medicare Patrol, Indiana Association of Area Agencies on Aging, Indianapolis, Indiana	44
QUESTIONS FOR THE RECORD	
Kathy Stokes, Director, Fraud Prevention Programs, AARP Fraud Watch Network, Washington, D.C.	48
Scott Pirrello, Deputy District Attorney, Head of Elder Abuse Prosecutions, San Diego District Attorney's Office, San Diego, California	49
Susan Whittaker, Administrative Assistant, Lehigh County Aging and Adult Services, Allentown, Pennsylvania	68
STATEMENTS FOR THE RECORD	
America's Credit Unions Testimony	71
Defense Credit Union Council Testimony	73
Stop Scams Alliance Testimony	74
Dr. Stacey Wood Testimony	80

**FIGHTING FRAUD:
HOW SCAMMERS ARE STEALING
FROM OLDER ADULTS**

Thursday, September 19, 2024

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

The Committee met, pursuant to notice, at 10:02 a.m., Room 106, Dirksen Senate Office Building, Hon. Robert P. Casey, Jr., Chairman of the Committee, presiding.

Present: Senator Casey, Blumenthal, Kelly, Warnock, Braun, Rick Scott, and Ricketts.

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

The CHAIRMAN. Well, good morning, everybody. The Senate Special Committee on Aging will come to order. Welcome to the Aging Committee's hearing entitled, "Fighting Fraud: How Scammers Are Stealing From Older Adults."

Every year, this Committee conducts a review of the scams that target older adults, culminating in this annual hearing and the release of the Committee's Fraud Book. Here is this year's edition of that book, "Fighting Fraud: Scams to Watch For." I am grateful to work with the Ranking Member, Senator Braun, on this and the Committee.

This Fraud Book is a great resource for older adults looking to prevent fraud, featuring tips that will help them identify a scam and resources for those older adults who have been scammed.

Today's hearing will not only discuss fraud prevention in the tips highlighted in the Fraud Book, but also how the Federal Government and law enforcement agencies respond to reports of fraud. The scams that are perpetrated against older adults today seem similar to scams that have been around for a number of years.

We have all heard of these, unfortunately, and so many families have been the victims of them. Grandparent scams where a scammer pretends to be a grandchild calling in need of financial help. Investment scams, government imposter scams, lottery scams, tech support scams are just a few of the scams highlighted in our Fraud Book.

However, over the past few years, scammers have gotten increasingly sophisticated in how they contact and prey on their targets. With the advent of artificial intelligence, that we all know is AI, scammers can now make their messages both online and over the

phone more convincing. Email or computer pop-up scams used to be more easily identifiable, but now are much harder to detect.

In some cases, scammers go as far as cloning the voice, and we have testimony in this hearing or this Committee to that effect, cloning the voice of a loved one to convince the target of their veracity. It has become nearly impossible to tell whether the person on the other end of the line is legitimate or a scammer.

That may explain why recent FBI data shows that fraud losses among older adults have gone up in recent years, reaching \$3.4 billion in 2023. Leaders in scam prevention and education like AARP are racing to keep up with these trends and continue to educate older adults.

Meanwhile, law enforcement is facing an uphill battle when it comes to responding to reports, investigating, and identifying the perpetrators, and so many other challenges. I am thankful that we have Scott Pirrello, who is here today, who can share more about the work he is doing to fight fraud as Deputy District Attorney in San Diego, but we have got a lot more to do.

We need to continue to alert older adults about the scams they may be targeted with, and we need to work together across all levels of Government to identify and root out these bad actors. I will just change that and say criminals. That is what they are. Furthermore, we need to help those who have been victimized by scammers.

Earlier this year, I released a report called, "Scammed Then Taxed," detailing how the 2017 tax bill repealed a longstanding tax tool that helped scam victims avoid more losses. Older adults disproportionately use what was known as the casualty and theft loss deduction.

My report highlighted the crushing financial blow that this law dealt to scam victims, leaving them paying heavy taxes on stolen retirement savings. On top of financial losses, this experience can be emotionally devastating and isolating.

I am grateful to have Susan Whittaker from Lehigh County in Pennsylvania here with us today. Susan will be sharing her and her husband's experience with tech support scams. Susan's testimony is critical for us to hear today.

It is important for older adults across the Nation to know that they are not alone if they lost money to a scammer. I am pleased that the Aging Committee can shed light on these stories, and I will now turn to Ranking Member Braun for his opening remarks.

STATEMENT OF SENATOR MIKE BRAUN, RANKING MEMBER

Senator BRAUN. Thank you, Chairman Casey. If you listen closely, it is worth repeating, \$3.4 billion. That is what scammers got out of American seniors in 2023. They are coming from all kinds of places, Mexico, China, lot of African countries. One of these criminals that they received the money, it is basically gone.

Almost impossible to get it back. They impersonate others, fabricate stories, make false promises. Many different ways, and the only way is to prevent it once it just starts to occur. That is why we need to prioritize education and outreach so older adults recognize these red flags immediately.

Our community banks and credit unions are often on the first line of defense, intervening where they can see from their own past experience if something looks askew. My home state of Indiana, one community bank already has avoided \$1.2 million. In one community bank, that is a lot.

Local law enforcement also play a crucial role in scam prevention by investigating these cases, alerting the public of something that is out there. Scammers are always looking for that next loophole, including Federal programs, because this place has got so much money, so many programs, and is probably the defenseless of anything out there.

We have talked about the fraud in Medicare alone, which is astounding the amount of money, \$60 billion due to fraud, errors, and abuse—most of it fraud. Every dollar lost to fraud is a dollar that can't be spent on what the program is intended to do. In these scams, Medicare numbers are used to purchase medical equipment that a senior doesn't need.

This leads to additional co-payments and out-of-pocket costs and can use up any enrollee's benefits faster. Medicare fraud directly hurts taxpayers and individual seniors, and we are still trying to figure out exactly how pervasive it is because there is so much spent in that category.

In March, I led a letter to the GAO requesting a full audit of Medicare fraud. GAO began that audit in July. This will be the most comprehensive audit in the history of Medicare, long overdue. The results will uncover just how much fraudsters are stealing from the American taxpayer in one of our programs that is so important, along with Social Security, Medicaid, and ironically the three that drive some of our structural deficits anyway.

We can't afford one penny of fraud. We know that CMS can do more to stop fraud, and we are going to keep pushing to see that they do it. I introduced the Medicare Transaction Fraud Prevention Act with Senator Cassidy, which empowers CMS to conduct a fraud detection pilot, utilizing AI to detect scams so that CMS can quickly alert the Medicare beneficiary.

Similar to what credit card companies do. They are pretty good at it because that is the place where most fraud occurs in our country. The 2024 Fraud Book highlights many of the scams targeting older Americans and provides information on how to recognize the red flags. Anybody out there listening, get a hold of your representative, your Senator, and get a hold of this because it is the best, probably small, sharp, concise book that can give you a heads up.

Look forward to hearing from our witnesses so we can learn more about it, and I yield back, Mr. Chairman.

The CHAIRMAN. Thank you, Ranking Member Braun. Now we will begin witness introductions, and after those we will go to the testimony, but we are pleased to introduce our witnesses.

We are grateful they are here, having traveled here to provide testimony. Our first witness is Kathy Stokes. Ms. Stokes is the Director of Fraud Prevention Programs with the Fraud Watch Network at AARP. She leads AARP social mission work to educate older adults on the risks that fraud presents to their financial security.

Ms. Stokes, thank you for sharing your expertise with us today. Our second witness is Mr. Scott Pirrello. He is the Deputy District Attorney and head of Elder Abuse Prosecutions in the San Diego District Attorney's Office in San Diego, California. Mr. Pirrello, thank you for sharing your expertise and traveling here today.

Our third witness is a Pennsylvanian, Susan Whittaker. Ms. Whittaker is the Administrative Assistant at Lehigh County's Office of Aging and Adult Services in Allentown, Pennsylvania. That is on the Eastern side of our State, not far from the New Jersey, Pennsylvania border.

Ms. Whitakker's late husband, Bill, was the victim of a scam in 2022. We are grateful, Susan, for you being here today and for sharing your story and Bill's story with us. I will now turn to Ranking Member Braun to introduce our fourth witness.

Senator BRAUN. It is my pleasure to introduce Nancy Gilmer Moore. She is a Program Director for Indiana's Senior Medicare Patrol. Ms. Moore's work has been nationally recognized.

She received the 2023 Barbara McGinty Award for her distinguished service as a champion for all in the fight against health care fraud. Ms. Moore is a graduate of Indiana University and is dedicated to serving Hoosiers. Thank you so much for being here.

The CHAIRMAN. Thank you, Ranking Member Braun. Now, we will turn to Ms. Stokes for her opening statement.

**STATEMENT OF KATHY STOKES, DIRECTOR, FRAUD
PREVENTION PROGRAMS, AARP FRAUD
WATCH NETWORK, WASHINGTON, D.C.**

Ms. STOKES. Good morning. My name is Kathy Stokes, and I am the Director of Fraud Prevention Programs for AARP. Thank you for inviting me to testify on behalf of AARP at this important hearing, and I would also like to thank the AARP volunteers who are here with me.

This morning, I will shed light on the true impact of fraud, explain that anyone can be a victim and that it isn't their fault, and I will speak to the urgent need for a whole of society response to the fraud crisis. Through the Fraud Watch Network, AARP educates older adults on the risk that fraud poses to their financial security, meeting them where they are.

Hundreds of volunteers work with our State offices and communities across the country to equip older Americans to avoid fraud. We share information online through newsletters and a podcast, and we cover fraud in most editions of our publications that tens of millions of Americans receive.

Our victims support program includes a helpline that receives 500 calls a day. We also host support groups to address fraud's emotional impact. It is for people like Dave, who experienced a year's long romance scam through which criminals stole his home and his business. He lost his friends and family, and seriously contemplated suicide. The recent growth in fraud has been meteoric.

The FTC revealed that estimates of underreporting in 2023, suggesting that rather than \$9 billion reported stolen through fraud in one year, it is more likely closer to \$137 billion, and criminals don't discriminate. They target every demographic.

FTC data suggests that younger adults report theft by fraud more often than older adults, but when the older adults are victim-

ized, the financial impact can be catastrophic. These victims are financially ruined. They experience emotional and health impacts. Often their families are torn apart.

Many once financially secure, hardworking Americans are left to rely on Government safety nets. In my written testimony, I describe the sophistication and scale of today's fraud crime rings, but sophistication and scale alone aren't the reasons they succeed. Rather, it is because criminals know how to exploit the human brain.

AARP's own research unveiled that criminals know that to trigger a heightened emotional State is to bypass logical thinking. Criminals call it getting targets under the ether, and academics have shed light on the science behind it.

Linda, a college professor, shared her story with AARP about the day her life was turned upside down when a tech support scam that started with a fear inducing computer pop-up message led to a four-and-a-half month nightmare. It forced her to retire, and it saw her buying gold bars and putting them into a stranger's car. She thinks the whole experience could have killed her.

Becoming a victim is not the victim's fault. It is not because of their age or because of cognitive decline. They become a victim because criminals exploit how our brains function, and while there is no single solution to the fraud crisis, there are things we could all be doing that could help turn the tide.

For individuals, it is taking steps like freezing our credit and using password managers and multifactor authentication. For educators, focusing on the red flags is important, but so is training how most scams come at us and what to do when they do.

For industry, financial institutions must continue to innovate on fraud mitigation and tech companies must build safety and security into their product design and manufacturing, and industry and law enforcement must work together.

AARP is leading a public-private effort to enhance coordination through the formation of a national Elder Fraud Coordination Center, which should launch this year. Its origins linked to the FBI San Diego County Elder Justice Task Force, which has proven that gathering data on like cases creates actionable investigations and prosecutions.

I am honored to be at this table with San Diego's Deputy DA, Scott Pirrello, who directly supports the work of the Elder Justice Task Force. Policymakers can address fraud by supporting resources for State and local law enforcement, and full-time investigators for DOJ elder justice strike forces, reinstating the casualty loss deduction to address the taxation of stolen assets, legislation to limit the damage of crypto ATMs, and efforts like the National Elder Fraud Coordination Center.

AARP looks forward to collaborating with you on solutions to address fraud, and thank you, and I look forward to your questions.

The CHAIRMAN. Ms. Stokes, thanks very much. We will turn next to Mr. Pirrello.

**STATEMENT OF SCOTT PIRRELLO, DEPUTY DISTRICT
ATTORNEY, HEAD OF ELDER ABUSE PROSECUTIONS,
SAN DIEGO DISTRICT ATTORNEY'S
OFFICE, SAN DIEGO, CALIFORNIA**

Mr. PIRRELLO. Good morning, Chairman Casey, Ranking Member Braun, other members of the Senate Special Committee on Aging. Thank you for having me here. My name is Scott Pirrello, and I am a career Elder Abuse Prosecutor for the San Diego District Attorney's Office.

I had an epiphany in 2018 when I realized I was seeing zero scam cases. After some digging, I was shocked to learn that there were hundreds of reports that existed, but once local police departments determined that the scammers are far away overseas, the cases are discarded.

I assumed then that someone was in charge of working these cases. I was wrong. Right at this moment, thousands of seniors are being scammed by foreign nationals on the verge of having their lives destroyed. The most prevalent scam impacting seniors today starts with a pop-up message from Microsoft that asks the victim to call a spoofed telephone number.

The scammers, mostly operating from Indian call centers, convince those seniors to download remote access software authorizing the scammers to see inside their computers and ultimately convincing them that their bank accounts have also been compromised.

Victims are instructed that in order to save their money, they must withdraw tens of thousands of dollars in cash from their bank or purchase gold bars. They demand that cash be converted to cryptocurrency and sent through Bitcoin ATM machines or packaged up in boxes.

They are instructed to either ship the boxes across the country or they are told a courier will be coming to their house. This narrative is exactly what occurred in San Diego just last week. A 94-year-old Air Force veteran lost \$143,000 in five separate cash pickups over a two-week period.

Hundreds of thousands of victims fight through humiliation and shame each year and summon the courage to report that this has happened to them, but these victims are met with the most regrettable answer, I am sorry, there is nothing that we can do for you. We should all be ashamed of ourselves.

I am here today on behalf of the millions of elder victims and their families begging the Government, law enforcement, the banking and technology industries to help them. Existing programs are failing to impact the tsunami of fraud that we are seeing every day, and a national strategy is needed. We are failing the very people who need us the most, older adults, many of whom can't afford to lose anything, let alone everything.

Since 2019, on the backs of a few patriotic former Marines working in our DA's office in the San Diego FBI office, we have proven that something could be done to fight this siege. Instead of surrender, under the leadership of San Diego County's elected DS Summer Stephan, we worked with the San Diego FBI in 2021 to launch a first of its kind Elder Justice Task Force, or EJTF, to combat elder fraud.

We have since learned that scammers abroad depend on organized networks of money launderers within the United States, and there are thousands of criminals within these networks to bring to justice.

The EJTF consists of the DA's office, FBI, Adult Protective Services, U.S. Attorney's Office, local law enforcement, and our local fusion center, all working together to turn individual local fraud investigations into large scale Federal cases and also using Federal seizure warrants to recover millions in fraudulent funds for our victims, whether a criminal investigation is opened or not.

This is the only initiative in the Nation responding to elder fraud cases in real time by tracking each fraud report collected by local police, the FBI's IC3 data base, and APS. This active review of reports and constant contact with victims enables us to better understand how these transnational criminal networks operate.

We are disrupting these networks. We are routinely filing State prosecutions on couriers, which have resulted in Federal indictments, including July's indictment by the U.S. Attorney's Office of a money laundering ring responsible for receiving stolen funds from over 2,000 older victims, totaling \$27 million in losses.

The numbers are doubling in San Diego from 2002 to 2023 with \$98 million in losses. Investing in education and task forces are critical to fighting these scams. However, we can't educate our way out of this problem, nor can we prosecute our way out. We need a whole of nation strategy.

The cause of fighting elder fraud does not yet have a face. It is too siloed and unorganized. The U.S. Senate Special Committee on Aging should take the lead to ensure that not one more victim falls prey to these scams.

We can actually stop this problem. We can all do more for these victims, especially for the grandparents who are going to wake up tomorrow and turn on their computer and have a pop-up ad. What will our answer be tomorrow when those victims call us for help? Thank you.

The CHAIRMAN. Mr. Pirrello, thank you for your testimony. We will turn next to Susan Whittaker.

**STATEMENT OF SUSAN WHITTAKER, ADMINISTRATIVE
ASSISTANT, LEHIGH COUNTY AGING AND
ADULT SERVICES, ALLENTOWN, PENNSYLVANIA**

Ms. WHITTAKER. Chairman Casey, Ranking Member Braun, and members of the Special Committee on Aging, thank you for inviting me here today to hear my story. I am Susan Whittaker, an Administrative Assistant for the Executive Director of the Lehigh County Aging and Adult Services in Allentown.

I have been in my current position for four years. My previous position was 45 years at the Morning Call, a local newspaper. I am presenting testimony today because my late husband, Bill, was a victim of a scam. I will also share the steps I took once I knew the scam had happened and the unavailability of the bank we entrusted with our personal account and business account.

It was Tuesday night when I got home, and Bill was more quiet than normal. He did not talk for the next few days. Bill suffered from dementia and Alzheimer's, diabetes, congestive heart failure, pulmonary embolisms, and neuropathy.

At the time of the scam, he was 75. Although Bill had sold his business, Bill Whitaker and Son Construction, LLC to his son, Bill stayed on as the office manager. He took care of all office responsibilities. As the week went on, Bill seemed to be quieter, and he seemed to be worried.

On Friday night, he started to tell me what had happened. He told me he received an email from QuickBooks, which was used to manage bookkeeping for the business. The email said that the business account had been charged \$499 for an upgrade. He said he didn't order the upgrade.

He contacted what he thought was QuickBooks at that point. The person told Bill that in order for him to refund Bill's money, Bill needed to first pay him \$500, and then QuickBooks, who was really the scammer, would send it right back to him via another payment platform.

He was told not to share this with anyone because if he did, he would not get his money back. Bill was instructed to install an application on the computer so he could transfer the funds directly to the scammer's checking account.

Bill also scanned and sent him a copy of his Social Security card and driver's license. Once everything had been set up, the scammer told Bill he would set up a Venmo account. He walked him through the process.

Finally, he showed Bill how to transfer the \$500 via Venmo. Because the scammer had access to the computer as Bill was in the middle of typing the number 500, the scammer took control of the software and added an extra zero. \$500 became \$5,000. He started yelling at Bill for making such an error when in reality Bill had not made a mistake. He said that now Bill needed to send him the \$5,000 in order for him to send back \$5,000.

That Friday night, Bill shared with me, in addition to the \$499 initial fraudulent upgrade fee that needed to be refunded to the business account, this individual now owed us money from our personal account due to the numerous Venmo transfers.

Bill said that this individual would be calling him back tonight at 6.00 p.m. This time I answered the phone. The scammer was totally surprised to hear from someone other than Bill. I questioned the process he had put Bill through. I knew it was a scam, but I asked him to please check with the boss. He said he would call me back.

At that point I wasn't even sure how much money had been taken from our accounts. While waiting for the call back, I shut down the Mac and booted it back up. I created a new login account and deleted the old information. I found the software that was installed and uninstalled it.

I also contacted our bank, Truist, through their customer service department. Since it was after 6.00 p.m., customer service was closed until Monday morning at eight. Then I called their fraud number. They too were closed until Monday morning.

Bill called the bank manager at the local branch and asked for help. The branch manager said he would do what he could, but he wasn't sure he would be able to get any of our money back. Monday morning, Bill called local law enforcement. He spoke with him, and

they said they would be in touch with the bank and would work with them.

The person Bill spoke with was very kind and patient. During that time, I put a stop on all credit reporting, a hold on all accounts, and called the Truist headquarters in North Carolina. I never did get to speak to anyone.

In the end, the scammer took a total of \$28,000 from us. However, the bank, along with the law enforcement, recovered \$8,000 of the money taken from our accounts, because they acted so quickly, they were able to stop the funds before they were dispersed. Despite this, we still lost \$20,000.

The scam was devastating and had a devastating effect on Bill, both financially and emotionally. Because we lost \$20,000 and Bill had a lot of chronic health issues, he began to ration his medications. We just couldn't afford them anymore.

Bill also felt responsible and felt that he owed it to a son to repay the money. He kept saying he was sorry and that he was stupid. He asked, how could he make such a stupid mistake. I assured him that he was only trying to save \$499 from the business and that he didn't do anything wrong. For several days he was very quiet.

After the scam, Bill would not answer the phone unless he knew the number and he would not open his email unless I reviewed it. Bill started to doubt himself in everything he did. His son no longer allowed him to do any work for the office, and so Bill lost his job. He also lost his sense of self-worth.

I was really—it was really sad to see this very intelligent and past business owner become so afraid to read emails and use the phone. It was a huge setback for him, and I think contributed to his worsening health conditions. Thank you.

The CHAIRMAN. Susan, thanks for your testimony. I know it has to be personally difficult to relive that and we are just grateful you are willing to do it—to testify in a manner that will help others, so we are grateful for that.

Ms. WHITTAKER. Thank you.

The CHAIRMAN. Finally, Ms. Moore.

**STATEMENT OF NANCY GILMER MOORE, PROGRAM
DIRECTOR, INDIANA SENIOR MEDICARE PATROL,
INDIANA ASSOCIATION OF AREA AGENCIES
ON AGING, INDIANAPOLIS, INDIANA**

Ms. MOORE. I would like to thank Ranking Member Braun, Chairman Casey, the other witnesses, and all in attendance for giving me this opportunity to speak about Medicare fraud and scams that target older adults and people with disabilities.

As the Indiana Senior Medicare Patrol, or SMP Program Director since 2013, I have learned that one of the biggest crimes affecting older Americans and people with disabilities is Medicare fraud, waste, and abuse.

In addition to Medicare's own provider focused fraud prevention units within the Centers for Medicare and Medicaid Services, or CMS, the U.S. Administration for Community Living, ACL, funds and supports the beneficiary focused Senior Medicare Patrol Program.

With programs in every State, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands, SMP's purpose is to edu-

cate beneficiaries, caregivers, and professionals on how to prevent, detect, and report Medicare fraud.

CMS offers no official estimates of total yearly Medicare fraud, but health care experts estimate improper Medicare payments are approximately \$60 billion per year. The U.S. Department of Health and Human Services Office of Inspector General, OIG, most recent annual report indicated that SMP projects reported more than \$111 million in expected Medicare recoveries in 2023.

Our Indiana SMP uses volunteers and in-kind members in partnership with most Area Agencies on Aging four senior centers and a center for independent living to help us educate people about fraud, errors, and abuse in Medicare.

Our partners give public presentations, exhibit at Health and Senior Fairs, and provide individual counseling across Indiana. We also regularly publish statewide social media updates, generate earn television and print media through relationships we cultivate with local investigative reporters, and periodically conduct SMP marketing campaigns.

We also collaborate with organizations through a coalition we founded with the Indiana Secretary of State's Office called the Indiana Council Against Senior Exploitation or INCASE. Members include the Indiana Secretary of State's Office, the Indiana Attorney General's Office, State Health Insurance Assistance Program, or SHIP, the Social Security Administration, the Internal Revenue Service, the Indiana State Police, financial institutions, and many others to conduct joint presentations about Medicare fraud and other financial scams that target older adults.

SMP programs across the country can provide early detection and warning of emerging frauds and scams. Here are some examples of suspected fraud that the Indiana SMP reported to the OIG during the past year.

In the intermittent urinary catheter fraud scheme, most of the beneficiaries noticed billing for urinary catheters on their Medicare statements that they and their doctor neither ordered, needed, nor received.

Many were billed for multiple months, with Medicare paying about \$1,500 per month for each separate billing. I personally noticed billings for urinary catheters on my own Medicare statement for May and June and promptly reported the suspicious claim to CMS and requested a new Medicare number since mine was compromised.

Durable medical equipment, or DME fraud is a perennial scam which includes all types of orthotic braces. Beneficiaries continue to contact Indiana SMP reporting unsolicited calls identifying themselves as representing Medicare with an offer for free orthotic braces.

The scam often begins with an initial contact from a call center, which makes a referral to an unscrupulous doctor or telemedicine company and a final referral to a DME provider. The braces delivered are often inferior and the beneficiary's personal doctor is not typically notified nor consulted.

The Indiana SMP recommends that all Medicare enrollees and their caregivers review their Medicare summary notices or MSNs for Medicare fee for service or explanation of benefits, EOBs for

Medicare Advantage plans. Beneficiaries should be on the lookout for duplicate billing, services or products not rendered or received, and services not ordered by their physician.

We also remind beneficiaries and caregivers that they should never give their Medicare number or financial information over the phone to unknown caller and that Medicare does not make unsolicited phone calls.

Ensuring the financial integrity of Medicare is essential to the millions of Americans who currently depend on it to access comprehensive health care services, as well as thousands of people who become newly eligible for Medicare every day.

As U.S. citizens, we all need to become better, more conscientious health care consumers, and help identify any potential improper payments. To that end, we have supported Senator Braun's and this Committee's work to reduce or eliminate Medicare fraud.

We assisted Senator Braun's office with the development of his Medicare Transaction Fraud Prevention Act, which would enhance the Medicare fraud prevention system to alert the beneficiary being scammed.

Thank you for allowing me this opportunity to share my experiences with you today.

The CHAIRMAN. Ms. Moore, thanks very much for your testimony. We are going to move to questions. I will start and then I will turn to Ranking Member Braun. I want to start with Susan Whittaker.

Susan, I want to again thank you for providing not just testimony but sharing your personal experience that you lived through, and your husband lived through, and the loss you suffered, both the financial loss, as well as the loss of your husband.

You had shared, and I think one of the words that come to mind are red flags. You would share with us that you could identify some of those red flags, I guess mostly based upon your work with the Lehigh County Office of Aging and Adult Services, which is for that county the Area Agency on Aging.

Your work helped you recognize some of these red flags when Bill shared what had happened during the scam. We know that education, providing information from, for example, our Fraud Book is critically important.

We wanted to make sure that we not only had a Fraud Book, but we have two versions of it. The one on my right is in English. The one on my left is in Spanish. More will make reference to the Fraud Book again, but we want folks to know that you can receive this information. You can go to our website at aging.senate.gov/scam. I will say that again for people that are listening, you go to the Aging Committee's website at aging.senate.gov/scam.

We want to make sure that people can avail themselves of this information. This isn't limited to one category of Americans or one age group. This can happen to anyone, and it is always easier, of course, after the fact to review what happened in a case and say, oh, I would have noticed that. Maybe not. No matter what your age and maybe not, and so, we have all got to be made aware of these scams.

Susan, I wanted to ask you, tell us about the red flags that you spotted because you walked us through a very detailed summary of how Bill was drawn into this, and then once he started telling

you about what happened, you were able to act and to be able to, I guess, counteract what the scammer was trying, so tell us what were the—you don't have to walk through every red flag, but just examples of red flags that you identified and can be helpful for us to know about.

Ms. WHITTAKER. The first red flag was when Bill said that he wasn't supposed to tell anyone, or he wouldn't get his money back.

The CHAIRMAN. Right.

Ms. WHITTAKER. My background at the Morning Call and also at aging technology, we do constant tests, if you will, on scams and phishing, and anyone that might be searching for information, so that is one of the things that is highlighted for the training—that was highlighted in the training in both areas. The other thing was, if you knew Bill, he was so detailed. I mean, he would spend four days trying to find out where a penny belonged in the checkbook, so for him to make an error and add a one—you know, add a one in front of the 500 or an extra zero at the end, that—he would have never done that. That just wouldn't happen, so that was the second one.

The more Bill talked about the steps that went through, and when he told me that they had him install software and open a Venmo account. In order to open a Venmo account, they needed his driver's license and Social Security number, it was just—it had just gone further than needing to refund the \$500.

Not only that, if the charge was \$499, why would you send us 500 back? It didn't make sense to me.

The CHAIRMAN. I think they are all—we all learned from that from that story and your identification of those red flags, and so you—and I guess your experience with both the Area Agencies on Aging of the Aging Office, but also working for a newspaper that—I guess that helped as well.

Ms. WHITTAKER. Yes.

The CHAIRMAN. I wanted to move next to—and I will turn to Ranking Member Braun, but because it is a busy Thursday, we will have Senators in and out, popping in, asking questions, coming to appear but maybe not able to stay to ask questions.

We will maybe take some extra time at the beginning here, but I want to turn to Kathy Stokes and Scott Pirrello.

Ms. Stokes, you talked in your testimony about how society frequently places blame on the victims for falling for the scams, and that alone has to add considerable trauma to the experience. The stigma associated with being a scam victim discourages many older adults from reporting.

I think that is probably an understatement. Really low reporting levels, I guess. It is critical that this information is reported to the relevant agencies. I ask you this, why is it important for older adults to report frauds and scams that happened to them?

Ms. STOKES. Thank you for the question, Senator. The reporting is critical. For one thing, it does help people who are in investigations see what is happening and tie cases together. I think it is even more important because it will then help law enforcement and policymakers understand just how big this problem is.

I had mentioned the FTC data that suggests that rather than a \$9 billion amount of theft in 2022 I believe it was, they extrapolate

underreporting that it was \$137 billion. If we are not reporting it, we can't do much about it.

The CHAIRMAN. Yes. You know, one of the best things we can do is just to continue to encourage people to report.

Ms. STOKES. Yes, absolutely.

The CHAIRMAN. As well. Mr. Pirrello, I wanted to ask you the same question. You know, what can you add to this based upon your work through the—you know, from the vantage point of law enforcement?

Mr. PIRRELLO. Thank you. Thank you, Chairman. There is disorganization within reporting. Without a mechanism for centralized reporting, the policymakers are making uninformed decisions on where to allocate resources.

There are a multitude of places that victims can go to report their crimes, and we know there's incredible data from the FBI, and the FTC, and a dozen other sources, including this own Committee's fraud hotline number. The problem is there is no body that is consolidating all that data.

There is no organization that is looking at the local police reports in each jurisdiction, and the huge void that we encountered and confronted in San Diego was the Adult Protective Services data from around the country represents a huge missing piece because they are getting unreported cases from mandated reporters. The financial institutions are referring cases to APS.

When you combine all those numbers like we have done in San Diego, you get the number of actual reported fraud. The problem is, as Kathy Stokes has mentioned, is you have to add a multiple to that. We know from all our work in the elder abuse community that we are only capturing one in twenty cases total.

The FTC numbers were the first numbers to really provide that estimate.

The CHAIRMAN. That is helpful. I know I went over because we are waiting for some folks, but I want to turn to Ranking Member Braun.

Senator BRAUN. Thank you, Mr. Chairman. I want to start with Ms. Moore. Congratulations on what you have done back in Indiana. The acknowledgment that you are ferreting out fraud in our own State.

You know, that estimate and what it is, it was Senator Rick Scott and I and J.D. Vance that commissioned the GAO to find out what it is exactly. I know that will be helpful because we can see there is a wide range of what it might be. One thing that really caught me by surprise that there could have been one particular category, it was urinary catheters.

That there was enough information to—that was pretty well, you know, right under \$3 billion, so in Indiana, did we get hit by that as well? Then tell me what you know about that particular fraud? What are the other top two or three frauds involving Medicare that you have personally dealt with?

Ms. MOORE. Thank you for your questions, Senator Braun about Iran. The urinary catheter fraud is still being investigated, is my understanding, so that we have had about 40 cases reported to us.

Again, if people don't—since you didn't receive any product, the only way you would know is to read your summary notices, and a

lot of people don't read those. They are confused by those, or they just, if they don't owe any money, they are not prone to report it, so it kind of goes under the radar.

Senator BRAUN. Did we have any that you actually caught in our State? In other words, and it is clear that there will be a lot of unreported because \$2.7 billion would mean then that certain States are doing a pretty good job at it and many other States aren't, because that is a huge figure.

That is why I was curious in our own State, since it doesn't sound like there were that many, maybe just 40, did many actually lose money out of those 40, or did you just hear about it and then prevent it?

Ms. MOORE. No, we reported it. Most of it was after—the Medicare had already been—

Senator BRAUN. Billed and the money had gone?

Ms. MOORE. Yes. Because it comes on your Medicare statements, which if you don't have a Medicare.gov account online, you know, it takes—they are only mailed about once a quarter, so you wouldn't—like I said, nobody received the product. In my own case—

Senator BRAUN. In Indiana, not counting what wasn't maybe reported, but what was reported, we had kept that down to a fairly small amount because that wouldn't—that would be such a small fraction of \$2.7 billion.

Ms. MOORE. Correct. Some people were billed for as many as 12 months or 10 months, because in Medicare, you can bill I think up to a year, you know, retroactively, so.

Senator BRAUN. I am a big believer that best practices among States ought to be shared. It sounds like you are doing a heck of a job. You have been acknowledged for it.

It seemed to me, Mr. Chairman, that we would want to find out what other enterprising States are doing, and that would be one way to share stuff that is already working, so what are the two or three other scams in Indiana that seem to be most prevalent?

Ms. MOORE. The most recent scams we are hearing about—and we are still getting, the DME braces scams and Medicare card saying you need a new Medicare card. One of the new recent ones is the caller—it is an impostor call saying they are from CVS, the large pharmacy chain, and that they—you can order your diabetic supplies through them.

We have only had a few cases of that, but I have connected with my SMP colleagues throughout the country, and they are seeing this as well. CVS does have a disclaimer on their website that this fraud has been prevalent.

Another one which is very similar to the urinary catheter fraud is people are being billed for ostomy supplies, which ostomy is any kind of artificial opening like colostomy or tracheostomy, and people are getting billed for that as well. We are seeing that in many other States throughout the country.

I think one of our big—what has helped us is having investigative reporters do stories for us because that really gets people's attention.

Senator BRAUN. Well, good. Thank you for the good job you are doing back in Indiana. I would be interested to see how you keep

track of it, and maybe over the last couple three years, what we have actually gone on record in terms of true laws in our own State. I like that idea of sharing what we are doing with maybe other States. I yield back for now. Thank you.

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

Senator Rick SCOTT. Well, first, I want to thank the chair and ranking member for doing this. I mean, this a significant issue that is impacting all of our States.

I want to thank you for holding the hearing and I want to thank you for putting this book together. Hopefully it is going to help a lot of people not get scammed. First, Ms. Stokes, you mentioned in your testimony transnational criminal organizations are behind many of the modern scams.

Are there in any particularly favored countries these transnational criminal organizations use and hide in to evade U.S.—our prosecution?

Ms. STOKES. Well, thank you for that question. I think maybe Scott would be better able to, from a law enforcement perspective, speak to it. What we know from our own experiences, big places are India, Africa, Costa Rica, Jamaica, Canada, and a lot of territories in Southeast Asia currently, including Myanmar, Cambodia, Philippines.

Senator Rick SCOTT. Scott, do you want to add anything?

Mr. PIRRELLO. Thank you, Senator. I echo what Kathy said, yes, that there is threats abroad. Right now, the most prevalent scams are tech scams that originate from Indian call centers.

The issue with enforcement is, is even if we had the capability to shut a call center down, they could obviously close up shop and move across the hall and start calling again, which is why the idea of a whole of nation strategy is really what would be impactful, because you have to look at the scam and then every point either upstream or downstream of the scam to see where we could stop it.

If we could focus on how the Indian call centers, for example, are contacting our victims, that would be a way to significantly slow or stop the scam activity because they are using our own technology against us.

Senator Rick SCOTT. Right. Do either of you have any sense whether the State Department is doing anything to prioritize this with regards—because take India, that is supposed to be an ally. Is the State Department doing anything to address this with the Ambassador or anything?

Mr. PIRRELLO. I do know that the Department of Justice and the FBI has attaches in these countries, and they are working and there are some successes to report on. Unfortunately, we obviously have our finger in the dam.

Senator Rick SCOTT. Yes. For any of you with recent breaches in personal information, there could be an explosion of identity theft as millions of people's names, dates of birth, and Social Security numbers become available to criminal networks.

How can we educate seniors to protect themselves and monitor their information for potential identity thefts that could result in loans or credit cards being taken out in their names? I don't know if any of you would answer that.

Ms. STOKES. Thank you, Senator. You know, we at AARP tell people, you know, your data are already out there. What we are seeing is just more and more of the same, and we all should be doing is taking steps to sort of shut it down in the ways that we can, and one of the most important ways is to freeze your credit reports.

That way, somebody who tries to use your identifying information to open credit against you is not able to do that, by and large. Really, really important is how we deal with passwords. You know how difficult it is to have, you know, 12-digit passwords for your 50 online accounts.

I find the password manager, once you kind of figure it out, is potentially a better way to deal with that, because if a criminal gets hold of a password that you use over and over, they are going to take over each account.

Another thing is multifactor authentication and shredding. I mean, it is online, and it is in—you know, it is in the real world too. Shredding your documents continues to be very important.

Senator Rick SCOTT. Scott, you want to add something?

Mr. PIRRELLO. Thank you, Senator. I think a distinction does have to be drawn. Identity theft is a massive problem, and it is an incredible inconvenience for our victims.

However, in a lot of cases, when there is a victim of identity theft, there are remedies through the banks, through financial companies that will recognize that someone has been the victim of an identity theft that they had nothing to do with.

With elder scams specifically, our victims are really left with nothing. They go to their financial institutions, and they are told that they are out of luck because they walked into the bank themselves and withdrew the money, and there is no remedy available to them at all.

Really, when you understand the nuance of these scams and understand that the scammers in the most popular tech scam that I have described, the scammers actually tell our victims to keep their phone on and put it in their purse when they walk into the bank. They are being listened to by the scammers.

There is a distinction, I think, between the identity theft and the elder scam victim.

Senator Rick SCOTT. Well, thanks each of you for being here, and again, I want to thank the ranking member and the chair for putting this together.

The CHAIRMAN. Thank you, Senator Scott. We will turn next to Senator Ricketts, if you—

Senator RICKETTS. Great. Thank you, Mr. Chairman—

The CHAIRMAN. We have other Senators on their way, so as people—

Senator RICKETTS. Well, if they are not here, they don't get to go.

The CHAIRMAN. You can—jump right in. Jump right in.

Senator RICKETTS. All right. Good. Thank you very much, Mr. Chairman. Well, as we know, many seniors and vulnerable Nebraskans are faced with challenges of protecting themselves and their loved ones from the threat of fraud, abuse, and financial exploitation. Financial losses due to scams continue to rise, particularly among older Americans.

In 2022, consumers reportedly lost \$9 billion to scams, a 30 percent increase over the year before. Older adults reportedly lost over \$1.6 billion to scammers. Federal Trade Commission has reported a tenfold increase in bank scams in the last three years. Scammers are also taking advantage of complex health care and insurance coverage decisions by impersonating the Medicare program.

Last year, late last year, officials with Nebraska groups that managed care for seniors began noticing a sharp increase in billings to Medicare for urinary catheters. According to the Medicare data for One Health in Nebraska indicated that spending on these devices on behalf of their patients was up an average of \$60 per patient, totaling more than \$1 million.

The fall from the scheme and the harm done is still unknown. Many people affected by the scheme may not even be aware that they have been scammed. Ms. Whittaker, we know that elderly population is disproportionately targeted by malicious scam calls.

Do you believe in education awareness of how these scams work could better prepare those being targeted? How would you approach being able to make people aware?

Ms. WHITTAKER. Thank you. Absolutely, I believe that education is really important. We at the Area of Aging, we have put together posters, fliers, pamphlets, magnets, and we have a folder that we actually take out to each individual that we are going to see.

This information is right inside the folder, including the magnet. Who to call in case you are a victim of fraud, or you feel that there has been a scam taking place.

It includes the fraud hotline, the Attorney General's number, the local police officer, State police, I believe, is the phone number that is on there, and it walks you through the steps of exactly who to call and what to do.

Senator RICKETTS. How do you distribute that? How do you make people—how do you get that information out?

Ms. WHITTAKER. We have an advisory council and the advisory council members distribute some of that information for us. In addition, our assessors take a folder out of all of Aging's information to every individual that they see. One of our assessors may—I believe the assessors see about 200 people a week, if not more.

We are getting that out to at least 200 people, 800, 1,000 people a month. The assessors do walk through that information. If you are receiving a waiver or option support, that is also covered by those that are going out. Our Aging care managers are seeing them.

Senator RICKETTS. It is a very one on one type of education—

Ms. WHITTAKER. Very one on one. We also did a scam seminar for the public and for health care workers at DeSales University. That was just last—that was just this past year. I don't want to quote the month because I could be wrong, but we had a huge attendance.

I have learned that Scott's associate was the person doing—was one of the presenters. We had representation from the local banks, the District Attorney's Office, some of our own detectives, Aging. We held that and made that available to anyone that was interested in attending.

Senator RICKETTS. All right. Thank you. Ms. Moore, there is a long list of ways scammers can take advantage of seniors. Are there certain methods of scamming that are more prevalent in rural areas?

Ms. MOORE. Oh, thank you. That is a good question. I think most, you know, most scams start by telephone or text, whether they are rural or, you know, urban beneficiaries.

I do think the telephone, you know, communications, we need more safeguards, and calls can be spoofed and labeled to look like they are coming from a legitimate organization or with their area code and even prefix, so people tell me they are more likely to pick up.

We tell people not to answer unsolicited calls or calls they don't have in their phone or, you know, if they have a landline sometimes you can put in certain numbers. I would say the telephone is probably the worst offender. Senator Ricketts. Do you think, if in rural areas, are there different ways of outreach or education that we need to approach when we are thinking about how do we educate seniors in rural areas?

Ms. MOORE. That is something we as a program, we, you know, work on. I think print media is better in rural areas. I do think, you know, we try to get to the very small towns and counties in our State through just presentations through Area Agencies on Aging, or we have some senior centers.

I have one—one of our partners does—she sets up a table for SMP and other services that the triple-A offers in a free laundromat day for seniors. We need to think really outside the box, you know, maybe even hair salons and that kind of thing, to get to people that maybe aren't on the Internet, don't, you know, maybe see the news, and that kind of thing.

Senator RICKETTS. Yes. I appreciate that, because I think you are exactly right. Thinking outside the box about how you reach seniors in rural areas is an important thing to do. I would just emphasize what you said about print.

You know, those weekly newspapers that are in rural Nebraska, and I am certain in other parts of the country, they are read cover to cover, and they stay on the kitchen table or on the, you know, the coffee table for a week.

If you have an ad or a story or anything like that in those, that is a great way to reach the seniors because again, they are read cover to cover and they leave them out for the week until the next edition comes out. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Ricketts, thanks very much. I am going to do some questions now in a second round, because I know we have one, two—at least two or three more Senators that are kind of in transit. I wanted to direct these questions to Ms. Stokes and Mr. Pirrello.

As I mentioned earlier that we have had for, I guess, a century prior to 2017, the casualty in theft loss deduction that theft victims could claim a tax deduction to offset their loss when they are a victim of a scam or other theft.

That changed in 2017 with the tax bill. The theft loss deduction was changed. It was repealed. Now victims of fraud and scams can no longer deduct their losses. They owe huge tax bills on money

they will never benefit from, leaving many older scam victims to feel that they have been victimized a second time.

Earlier this year, as I mentioned in my opening, we released a report entitled, Scammed, then Taxed, and that legislation or that report outlined what had happened. Both of you work extensively with older adults, and you have tragically had the—those adults who have tragically had the entirety of their life savings stolen from them.

I will start with Ms. Stokes. Have you encountered times when older adult scam victims were surprised that they owed taxes on their stolen money? How does that affect them?

Ms. STOKES. Thank you, Senator. The victims that we have talked to personally through our helpline and through these online victim support sessions that we have, this is probably the thing that makes them the most anxious.

It is revictimization, plain and simple. They have had everything stolen from them, but the IRS sees that as income, and they tax them on it, and they don't even have the money to pay that tax. It is an issue of great anxiety for many people who are experiencing this.

The CHAIRMAN. I guess part of the challenge here is that sometimes tax professionals may not have been—they may not have updated their information about how the tax law changed and may not be telling people enough.

We have got to make sure that people know. I think the remedy here, of course, is to change the law back to the way it was and reinstate that deduction. Mr. Pirrello, how about your experience with this?

Mr. PIRRELLO. Thank you, Chairman. I have talked to several victims who have encountered this, and this is a result of the scammers elevating their techniques by having our victims not just drain their checking or savings account, but actually completely liquidating their 401(k) or retirement account.

We are talking about victims that have lost seven figures, as you said, the entire nest egg, and the timing of it is that they go through the trauma of losing everything in their life and they are just rebounding maybe six months, a year later, and their accountant tells them that they have a 1099 from their brokerage company that says they owe, for one of my victims, a \$300,000 tax bill.

I equated that to a gut punch at the end of this. There is another layer beyond that, because many of these victims have no recourse, that they have to go online and find a tax attorney that they have to pay tens of thousands in dollars to. There is another void just on the IRS's website, has a lot of information about identity theft. There is no direction.

Our elder scam victims are left bewildered. If they go to the IRS site, there is nothing for them to click on that says, you have been scammed. Here are some instructions to follow to get to this amazing program, the Taxpayer Advocate Service.

Most victims have no idea what that is, and they are just spending money and being scammed on top of scams. Yes, that is a significant issue for those victims that have lost the most.

The CHAIRMAN. Yes. I think the phrase you used, gut punch, is a good way to describe it. You know, it is bad enough to be a victim

of a scam, and then to get the gut punch of a tax bill where that was not happening before that change in 2017.

I will turn next to Ms. Whittaker again and Ms. Stokes. I said earlier that there is obviously an emotional impact that people experience, which is probably indescribable. I am going to be turning to Senator Kelly in a moment, but Ms. Stokes and Ms. Whittaker, you had made reference to your own experience, Ms. Whittaker's personal experience, and Ms. Stokes, through your work.

I mentioned the emotional turmoil that people experience generally, but then when they are hit with a tax bill, it is far worse. One of the victims that we described, talked about the scam as "an excruciatingly painful experience."

Another said, "when I found out I was scammed, I had suicidal thoughts". It is clear that these scams do far more than just take money from people. Ms. Whittaker, can you describe the feeling that you and your husband had when you knew that you are a victim of a scam? I guess he was a victim, and you were learning about it.

Ms. WHITTAKER. Devastation. Thank you. I was also angry. I have to admit that I was pretty upset with Bill, and he felt like he had really, really done something wrong when he was just really trying to save some money for the company.

He didn't want to be charged something he didn't order. Then afterwards, it was just—we were devastated. It was the needing to pay back the money to the business, which he felt was—he was responsible for losing to begin with.

I understand that it was the right thing to do, but it was just devastation.

The CHAIRMAN. Yes, I can't even imagine it. You know, and I will keep saying it, it is these scam artists, they obviously target seniors disproportionately, but it can happen to anybody. I will turn next to Senator Kelly.

Senator KELLY. Thank you, Mr. Chairman. Thank you for all of our witnesses for being here today to talk about a topic I think is sometimes uncomfortable talking about.

Mr. Pirrello, I understand from your testimony that the Elder Justice Task Force you helped create in San Diego is the first of its kind, bringing together local law enforcement, FBI, Adult Protective Services, and the U.S. Department of Justice.

I am impressed by the task force's ability to collect real time information and disrupt scams taking hold in your jurisdiction, especially ones that are originating overseas. I have gotten some scam calls myself from overseas before and, you know, have been personally tempted to take them on by myself.

However, I know it is best left to professionals like yourself for doing this, and you are proving that here. Mr. Pirrello, what is the key to the success of your Elder Justice Task Force?

Mr. PIRRELLO. Thank you, Senator. San Diego does have a proud tradition of collaboration between local and Federal authorities, and amidst all the local authorities, and I think that is the largest piece.

As we travel around the country and talk to people who want to duplicate what we are doing, you hear things like that people can't even get other colleagues from other agencies on a telephone call.

It requires people that view this issue with passion and are willing to sacrifice to get a task force like this up and running.

Senator KELLY. How do we—so, first of all, how much does it cost to operate your task force?

Mr. PIRRELLO. Well, it is interesting, Senator. Our task force started as a collateral responsibility for myself and every other member of law enforcement or the FBI, and so, there really wasn't a cost.

It was kind of a side hustle, so to speak, for many of us. Where the money needs to go is funding investigators, funding analysts. We need to fill positions. The law enforcement community is so starved for resources that it is very difficult to get any agency to dedicate a full body, a full resource to this.

Sadly, as you go around the country, there probably is not one single person in law enforcement anywhere, locally or federally, that 100 percent of their job responsibility is focusing on elder scams.

Senator KELLY. If it wasn't a collateral duty in your office and you were going to have dedicated people, how many people would be doing this?

Mr. PIRRELLO. Well, Senator, the numbers are staggering. As successful as we have been in San Diego, we are working less than one-tenth of one percent of the intake, to give you an idea of this tsunami of fraud that is coming at us.

We will take one body. We could use an army, obviously. It really takes, again, a group of people that is committed to this cause to start building it in each community. We started and we felt the best first step forward was identifying how big of a problem it was. It goes back to that underreporting and lack of centralized reporting mechanism.

As each jurisdiction, locally and then nationally, come up with the actual loss amounts in their own jurisdictions, that is the number that we need to go to the policymakers and decisionmakers to ask for the resources that this problem merits.

Senator KELLY. Yes. We can understand the amount of resources, I often think about this in terms of people. If you were going to stand up for your office, a team of people that were 100 percent dedicated to this, to actually handle the demand that you see out there, the fraud that is out there, how many people are we talking about?

Mr. PIRRELLO. You could get a task force started with one local prosecutor like myself, one investigator from the DA's office or from a local police or sheriff jurisdiction, and then cooperation from the local FBI office.

You could hit the ground running with the caveat that you need also the local U.S. Attorney's Office to devote the resources. The number one obstacle that we faced when we started our task force was the dirty word called thresholds within the criminal justice system. To get Federal Agencies like the FBI or the U.S. Attorney's Office to open up a case, typically, you needed million dollar cases.

Most of the cases, like unfortunately, Ms. Whittaker's family start by losing \$25,000, even \$300,000. You can't get the FBI or the U.S. attorney's office to open up that case. Our task force was devoted to working locally to connect the dots, to show our Federal

partners that these were million dollar cases once you connected the dots, but also for our local task force, the chain of command at the FBI and the U.S. Attorney's Office eliminated thresholds, which is a huge—was the only thing that got us really off the ground so that we can all work collaboratively on these cases.

Senator KELLY. I will take a couple more minutes. Another question on communications platforms, Mr. Pirrello. We had a hearing on this topic last November where we talked about how artificial intelligence plays a growing role in scams, both preventing them but also enabling them.

We talked about a constituent of mine who had received a phone call from somebody she thought was her daughter, and the daughter was screaming and crying, and a man came on the phone to say that he was going to do harm to her daughter if the woman didn't pay \$50,000.

Turned out that her daughter was safe at home, and this was just an AI created scam call using voice cloning technology. We learned in that hearing how difficult it is to trace and prosecute a scam if no money has been exchanged, which was the case here.

Mr. Pirrello, from the law enforcement perspective, why is that so challenging to trace and prosecute a scam if the scam wasn't completed?

Mr. PIRRELLO. Well, Senator, we believe that you have to devote your limited, scarce resources to where you can have the greatest impact. When we have talked to a victim and learned that they almost fell for this scam, there is great relief. As I mentioned before, the intake is coming at us faster than we could process.

Every single day we have victims that are losing tens of thousands of dollars or hundreds of thousands of dollars and our focus in the first days after someone has been scammed is not necessarily putting a bad guy in jail. It is, let's do everything we can to try to pull this money back from them.

On the artificial intelligence piece, that is great evidence that there is urgency here. We can't sit on the sideline any longer because AI coming, the scammers are going to be doing even better than they are doing now, and they are doing really well without the use of artificial intelligence.

When we look at the numbers, as Kathy mentioned, where the estimates of actual losses beyond what is reported is over \$100 billion a year. If that is how much the scammers are getting from us without artificial intelligence, this is the time.

The time is now. We are reaching a tipping point. We couldn't be more grateful for this Committee to take up this issue.

Senator KELLY. I read this article on CNN about a man in Virginia who was a victim of a pig butchering scam and met somebody online, convinced him to invest in crypto. He did it, never met her in person.

He lost his entire life savings and then he took his own life. The person on the other side of the screen, you know, wasn't just someone bored at home over the weekend. It was probably over in Southeast Asia somewhere—an organized crime outfit that is doing this at scale and it is very sophisticated. It is run by professional criminals, and they are getting older adults, as you mentioned, \$100 billion.

A lot of it is probably this, you know, this confidence investment scam, so what do we do about it? You know, how do we—you know, they are not going to stop. What kind of negative incentives can we put to the countries involved?

I know this isn't your area of expertise, but beyond just informing the public about this, I imagine for you it is hard to prosecute somebody that you don't know that is in a foreign country where we may or may not even have an extradition treaty, and it is hard to identify who these people are.

From a foreign policy standpoint, you have any ideas about what the Federal Government could be doing at the highest level to put pressure on the countries that are harboring these organized criminal groups?

Mr. PIRRELLO. Thank you, Senator. Sorry, thank you, Senator. I am actually—I am proud there is leadership coming from California, from San Diego, with our Elder Justice Task Force.

The Santa Clara District Attorney's Office is actually a national leader in combating the pig butchering scams, and Deputy District Attorney colleague testified in Congress yesterday on this issue I don't have an answer, a magic pill to solve that problem, but what I can say is when you do—when we are dealing with countries that are outside of the reach of United States law enforcement, I think the effort—and there are concrete steps that we could take, again, upstream of the scam to eliminate the ability for the scammers in Southeast Asia to contact our victims.

That is where resources should be spent and pressure on the technology industry. Every one of our victims is being contacted on a spoofed telephone number or a foreign IP address over the devices and technology that we depend on every day.

There are countries like the UK and Australia that have implemented programs specifically designed to eliminate that, and their trends are actually skewing downwards in the last two years. There is an addendum to my testimony that was submitted from the Stop Scams Alliance, who is led by a former CIA analyst, and there is some real concrete, specific things that the technology and communications companies can do, and so, if we eliminate the ability for these call centers to reach our victims, then we don't have to worry about the expense of chasing them to Myanmar or wherever else they.

Senator KELLY. All right. Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. Thanks, Senator Kelly. We obviously allowed extended time here, but Senator Kelly had a very important set of questions. I think this can lead to some good bipartisan work, and I hope we can stay in touch on this. I will turn next to Senator Blumenthal.

Senator BLUMENTHAL. Thank you very much, Mr. Chairman, and thank you for holding this hearing, and for this booklet, which I think will be very useful to a lot of my constituents, including the one in Spanish.

I want to thank Senator Casey for putting together these materials. Very important to educate people. Half of our job on topics that involve scams is to educate, enlighten, and warn people, including what law enforcement does, as I know from having acted

against these kinds of scams and con artists as State Attorney General, as well as United States Attorney in Connecticut.

Mr. Pirrello and Ms. Stokes, in your testimony, you both call attention to elder scams involving cryptocurrency ATMs. Along with Senator Durbin and a number of my colleagues, I wrote a letter to 10 of the largest Bitcoin ATM operators on their failures to prevent elder scams despite reports that criminals are coercing elderly Americans to make large deposits into these Bitcoin ATMs.

These companies have not taken any steps to ensure their ATMs are not being used in these scams. I would like to ask you, what do you think Congress should do to address elder scams involving Bitcoin ATMs and cryptocurrencies?

Ms. STOKES. Thank you, Senator, for that question. I know that the cryptocurrency vector is very, very concerning, so much is being stolen by convincing somebody that something is in—that something that isn't true and getting them to go to their bank, take out tens of thousands of dollars in cash, then telling them where to go to find the crypto machine, and then them standing there and putting \$100 at a time into these machines and coaching them on how to get that money to the electronic wallet of where they think that this is going to solve a problem.

It has just created all that much more—and I know that AARP State affairs are out there trying to get changes in crypto regulation. We do definitely need more regulation there, and some of the things that they are looking at are, you know, warnings about the fraud types that they are used in.

Transparency around the fees and the rates, and really importantly, I think daily transaction limits.

Senator BLUMENTHAL. Thank you. Mr. Pirrello.

Mr. PIRRELLO. Sorry—thank you, Senator. We did have a recent victim in San Diego who fell victim for the scam, withdrew \$15,000 from her bank and went into a liquor store in a part of town she shouldn't have been in the middle of the night to put \$15,000 cash into one of these machines.

I echo the sentiment, we have to have transaction limits, but we clearly need to look at this industry as a whole and how it exists, and what safeguards and accountability these companies should have. These companies are relying on the fact that our victims showed their driver's license to the machine, so they are complying with the know your customer requirements of their industry. However, clearly, these victims do not know what they are caught up in. They don't know where their money is going, and in this investigation that I just mentioned, we learned that our victim in Escondido, California put \$15,000 into the machine. Within 12 minutes of her putting her cash in the machine, money was taken from that Bitcoin wallet and placed on an overseas Bitcoin exchange that is outside the reach of law enforcement in the United States.

The window is so tight for there to be any intervention, and so there should be as many safeguards as possible to prevent these victims from putting their money in these machines in the first place.

Senator BLUMENTHAL. I take it from both of you that the companies themselves are doing virtually nothing to try to forestall this fraud.

Mr. PIRRELLO. Yes, your honor, they—your honor, I am a prosecutor. I am sorry, Mr. Blumenthal. Thank you, Senator.

Senator BLUMENTHAL. That is okay.

Mr. PIRRELLO. I mentioned earlier I was a career prosecutor. I can't turn that off. Thank you, Senator. The cryptocurrency, some are being responsible in the sense that they are submitting suspicious activity reports like a bank would, but as I mentioned, it is well after the fact that the victim's money is unrecoverable, and so both within our jurisdiction and around the country, there is frustration growing within law enforcement. We have a victim that runs to the police station and says, I just put \$10,000 into this machine and my money is sitting right there in that machine, can you get it back for me?

There is an inability to do that because of the nuance of how these cryptocurrency transactions work. Even a period of time, just like when you go to wire money, that there is a hold for 48 hours, just a brief period of time before that transaction takes place would save millions, there is no question.

Senator BLUMENTHAL. My time has expired, but I would welcome from you or any other members of the panel suggestions on how we can hold these companies accountable. The principle of accountability, I think, is very important.

They know it is happening. They could stop it. We need to make sure they do take action to stop it. I would welcome your additional written responses, if you have any. Thank you. Thanks, Mr. Chair.

The CHAIRMAN. Thank you, Senator Blumenthal. We will turn finally to Senator Warnock.

Senator WARNOCK. Thank you very much, Chair Casey, for your vigilance with protecting American consumers in so many ways and thank you for your focus on this topic.

According to the FBI's data on elder fraud complaints, elder fraud complaints, Georgia has the unfortunate distinction of being in the top 15 States for the number of complaints filed, and we are in the top 10 for the amount lost, almost \$92 million in 2023 alone. This data is stark and deeply concerning.

It is easy to get caught up in abstract numbers. Even a high number like \$92 million, what does that actually mean for folks who are paying attention to this hearing? So let me highlight a story to remind us of what is at stake. Behind the numbers are real people. My office recently heard the story of a Georgia senior who was a victim of a financial scam in which the scammer impersonated an Army office asking this Georgian for money to pay for his veteran's benefits.

Thankfully, her son, who is also a veteran, was able to prevent his mother from sending the scammer money, but it was a close call, and there are too many cases where these scammers take advantage of seniors. I have seen it up close as a pastor with members of my own congregation.

It can be difficult to talk about, but I believe the more we shed light on these deceptive practices, the more we can remove stigma and shame, and encourage people to report when something isn't quite right.

Ms. Whittaker, thank you so very much for being here, and could you talk about your own personal experience with scams and how it impacted you?

Ms. WHITTAKER. Okay. Financially—first of all, I think that the scammers do some sort of research. I am not sure what they use as the resource, but they clearly are doing research on their victims because they seem to know exactly what is available, and what is not available, and when to stop.

This started on a Tuesday, and Bill didn't say anything to me until Friday. Little chunks of money seem to be missing over the course of four days, which he was not aware of, and I wasn't aware of because he didn't say anything. It was in the end when we took a look at what was lost, and my father had just passed away, so we had some money from my dad, that fortunately—well, unfortunately was gone, but it saved us from actually having even more of a loss than what we already had, but because there was nothing left in our savings account or checking account, it affected decisions that had to be made as far as medicine that was Bill—was needed to take. You know, he chose not to take certain medicines.

Fortunately in the future I understand that some of those medicines will be taken care of, but he chose not to take Repatha which had an out of pocket, a huge out-of-pocket expense, but it was necessary for his cholesterol, but he wasn't going to take it.

He chose to not take all of his insulin. He should have taken insulin twice a day, in the morning and at night. He chose to cut those back from the number of units that he was taking until we paid the business back.

Once the business was paid back, and he felt better about where we were, then he started doing some of the things he should have done, but not all of them, so it wasn't just a financial effect, but he sort of stopped living, if I can say it that way. He was so ashamed of what he had done that he just made himself not available to people. I am not sure if I—

Senator WARNOCK. This—no, thank you. This scam had a material impact on your family.

Ms. WHITTAKER. It did.

Senator WARNOCK. Literally dragging the health of your father down as a result of it, and you know, not putting words in your mouth, it sounds like it—

Ms. WHITTAKER. My husband.

Senator WARNOCK. Your husband, sorry. Then entered the depression.

Ms. WHITTAKER. Yes. Depression, actually, for both of us.

Senator WARNOCK. Yes, yes.

Ms. WHITTAKER. It was—until you get—and then you reach a point where you just say, okay, enough is enough. You got to get up. You got to move on. I was able to do that. He was not.

Senator WARNOCK. Right, right. Well, thank you so very much. It takes a lot of courage to come to a place like this and tell your story, but I wanted folks to hear just a little bit of it, because I think sometimes, we get lost in the data and in the numbers. You are the human face of the issues that we must address.

I look forward to working with Chair Casey and the Committee to protect seniors and their families from the scourge of scams, and

Ms. Whittaker mentioned the ways in which our work separately on the issue of capping the cost of prescription drugs, my bill, which caps claims of insulin and other drugs, is helping seniors.

Even as we protect them from the big pharmaceutical companies and their excesses, we also got to protect our seniors from these scams. Again, thank you so very much for your testimony.

The CHAIRMAN. Thank you, Senator Warnock, and I appreciate you asking Susan Whittaker those questions. I am going to close now. We are at the end of our hearing, and we also have a vote coming up.

We just want to thank our witnesses for their testimony, the expertise they bring to bear, their own personal stories, and the wisdom you provide to the Committee to either change a law or remedy the policy that took away a deduction, but also to really begin to focus on what the Federal Government can do more of to combat this problem.

As you heard—for the audience I would say, as you heard from our witnesses, scam losses are on the rise. Fighting frauds and scams that target older adults is going to take a multi-pronged, whole of Government approach, and that means every level of Government.

I think the Federal Government can do more as we heard today. As Mr. Pirrello shared in his statement and in answers to questions, education and prosecution alone won't solve the problem, but we have to do both.

We need to hold all those involved, whether it is a bank, or a social media company, or any other perpetrator accountable, and ensure our law enforcement agencies have the resources they need to address this issue head on, and I think there is some—should be some good bipartisan work ahead of us on that.

We also need to reduce the stigma associated with these crimes. If you have been scammed, you are not alone. You are a victim of a crime. You should not blame yourself. If you have been victimized, please report this to our federal agencies without shame.

Without knowing the true scope of this issue, Congress can't provide Federal agencies with the resources needed to catch these criminals. We would urge people to report the scam as soon as possible to the FBI's Internet Crime Complaint Center, also known as IC3. That is letter, capital letter I, capital C, and the number 3, at ic3.gov, ic3.gov, or to the Federal Trade Commission at reportfraud.ftc.gov.

We will continue to amplify those resources for folks to turn to. We also need to support our older adults who have been scammed—with regard to the financial and emotional impact that we know is profound and the Federal Government should work to lessen that blow. Ms. Whittaker's testimony, she just made reference to a few moments ago about her husband, "stopped living in a sense." It says it all.

This means that we have got to work together to make sure that older adults who have been scammed out of their life savings aren't on the hook for the taxes for withdrawals associated with the scam.

I also will move to submit for the record the report that I made reference to earlier, Scammed, Then Taxed, which is a report about the change in the law that took away that deduction, and I will

also submit for the record a letter from AARP about the repeal of the theft loss provision.

Both the letter and the Scammed, Then Taxed report will be made part of the record, so ordered.

The CHAIRMAN. For those watching today, I want to emphasize that the Committee is here as a resource, whether you just want to learn more about this problem, or in fact, if you have been targeted by a scammer.

You can access our resources, including the Committee's newest Fraud Book with information, tips, and resources, and a helpful book bookmark with quick tips via the Aging Committee's website at aging.senate.gov/scam.

I will recite that again, aging.senate.gov/scam. Ranking Member Braun will submit a statement for the record and that statement will be added to the record, so ordered, when we have that statement.

The CHAIRMAN. I want to thank all of our witnesses once again for contributing their time and their expertise.

If any Senators have additional questions for the witnesses or statements to be added to the record, the hearing record will be kept open until Thursday, September 26th, one week from today.

Thank you all for participating. This concludes our hearing.
[Whereupon, at 11:39 a.m., the hearing was adjourned.]

CLOSING STATEMENT OF SENATOR MIKE BRAUN, RANKING MEMBER

Thank you to our witnesses for sharing your testimonies and personal experiences.

It's crucial that we examine the frauds and scams that target older Americans, and how to prevent these crimes through education and awareness.

Highlighting Medicare fraud is particularly important as it targets our most vulnerable populations.

Congress needs to address this with innovative solutions like my Medicare Transaction Fraud Prevention Act. Combatting fraud is a bipartisan issue.

I commend local banks, credit unions, law enforcement, and senior Medicare patrols for the work they do to prevent fraud and scams and educate seniors on what to look out for.

I appreciate our Committee's focus on this issue. I yield back.

APPENDIX

Prepared Witness Statements

U.S. SENATE SPECIAL COMMITTEE ON AGING
 "FIGHTING FRAUD: HOW SCAMMERS ARE STEALING FROM OLDER ADULTS"
 SEPTEMBER 19, 2024
 PREPARED WITNESS STATEMENT
Kathy Stokes

My name is Kathy Stokes, and I am the Director of Fraud Prevention Programs for the AARP Fraud Watch Network. I am honored to be here to testify on behalf of AARP, which advocates for the more than 100 million Americans age 50 and older. I would like to thank you and the members of the Senate Special Committee on Aging for holding this important hearing, "Fighting Fraud: How Scammers are Stealing from Older Adults." AARP has long worked to educate consumers, support fraud victims, and improve fraud detection and prevention at financial institutions, and we look forward to working with you towards policy solutions to prevent fraud and protect fraud victims.

AARP Fraud Prevention Work

The Fraud Watch Network is AARP's program focused on helping our nation's older adults understand the very real threat to their financial security that fraud represents.

We show up in communities around the country through all our state offices and their trained volunteer fraud fighters spreading the message of fraud prevention. We share robust information online at aarp.org/fraudwatchnetwork; we cover the issue in AARP the Magazine and the AARP Bulletin - which reach tens of millions of readers with each edition; we offer a biweekly email or text 'watchdog alert' newsletter and we produce an award-winning podcast, AARP's The Perfect Scam - in the true crime genre but focused on the impact of this type of crime on victims and their families. We also offer a variety of virtual educational events, from member teletown halls to webinars and Facebook live events.

Beyond education, AARP is unique in its focus on supporting victims of fraud and their families. Our Fraud Watch Network Helpline receives around 500 calls a day. These calls can be from people who simply want to report a scam they've encountered but didn't engage with, from people who aren't sure whether that Publishers Clearing House letter claiming they've won \$1 million and a Mercedes is legitimate (it's not), and too often, from victims and their family members in the aftermath of the crime. We also offer an online victim support group program, through which trained facilitators run small group sessions to begin to address the emotional impact of fraud victimization-helping older Americans rebuild their lives.

AARP has also been leading an effort to reframe the narrative on fraud victimization. Our society tends to treat fraud victims differently than other crime victims. We often blame them with the language we use: they've been tricked, or duped, or fooled, rather than that a criminal has stolen from them. We tend to believe that there's nothing law enforcement can do because the criminals are abroad. Our narrative change movement is rooted in research that shows how our tendency to blame fraud victims has served to deprioritize fraud as a crime. This must change if we are to meaningfully combat this insidious and devastating crime.

Additionally, AARP has been working as a convener to build support for a new nonprofit National Elder Fraud Coordination Center (NEFCC), which should launch before year's end. Similar to the National Center for Missing and Exploited Children, this private/public partnership will focus on sharing information to tie cases together for law enforcement investigation and prosecution to begin to disrupt the fraud business model.

NEFCC's origin links to the work of the FBI San Diego County Elder Justice Task Force, which has proven the concept of gathering data on similar cases to create high-dollar, actionable investigations and prosecutions. I'm honored to be at this witness table with Deputy District Attorney Scott Pirrello from the San Diego DA's office, who directly supports the work of the Elder Justice Task Force, especially when it has needed local prosecutions to assist federal investigations.

The Fraud Crisis

The growth in fraud crimes over the past five years has been meteoric. For example, published report data from the Federal Trade Commission (FTC) shows more than \$10.3 billion stolen in 2023; the Federal Bureau of Investigation (FBI) shows \$12.5 billion stolen in 2023; and Javelin Strategy and Research found \$43 billion in identity fraud scams alone in 2023.

But these numbers don't begin to tell the true story. In a 2023 report the FTC submitted to Congress, the agency acknowledged the significant problem of under-reporting. Using its own estimates of under-reporting, the agency extrapolated that money stolen from fraud in 2022 was not the reported \$8.9 billion, but more like \$137.4 billion. The agency acknowledges a considerable degree of uncertainty with this amount, but most fraud experts agree the higher number is likely closer to reality than \$8.9 billion.

Fraud criminals know no demographic bounds. They seek to steal money and sensitive information from targets regardless of age, educational attainment, or socioeconomic status, but when they victimize our nation's older adults, the financial impact is too often profound and life altering. This stands to reason, as older adults are more likely to have accumulated a lifetime of savings and are more likely to have housing wealth, and too often, the criminals steal everything. The victims are emotionally and financially ruined, often their families are torn apart, and many are left to rely on already strained local, state and federal safety nets.

Why Scams Succeed

The days of snake oil salesmen and lone grifters have given way to transnational organized crime rings with corporate offices, employees (often enslaved prisoners forced by physical threat to be frontline scammers), lead lists, personally identifiable information (PII) from data hacks and breaches, scripts, and a playbook of how to turn a fraud target into a fraud victim. These criminal enterprises leverage all methods of communication and forms of payment along with the latest technological advances to commit their crimes at scale.

But sophistication and scale alone aren't the reasons they succeed. The reason scams are successful is largely because of how the human brain functions. AARP's own research beginning decades ago unveiled what criminal scammers refer to as getting their targets "under the ether." They have known since the beginning of time that to trigger a heightened emotional state is to bypass logical thinking - it is how our brains work.

What criminals call getting the target "under the ether, academics refer to as an "amygdala hijack." The amygdala is the part of our brain that processes emotions. When the amygdala is hijacked, the part of our brain responsible for logic - the prefrontal cortex, is bypassed. It's important to recognize that becoming a fraud victim is not the victim's fault. They didn't become a victim because of their age, educational level or cognitive impairment. They became a victim because of how our brains function.

This message is critical if we are ever to marshal a meaningful response to the fraud crisis. Until we all understand that fraud victims are crime victims and that they aren't responsible for becoming victims, we will fail to address this crime for the scourge it is.

Concerning Fraud Trends

The tactics of fraud criminals range from old school (stealing your mail) to high tech (hacks of banks, retail chains and other companies that stockpile consumer data). They might pretend to be from the government, utility companies, banks or big tech firms to steal sensitive personal information, or they send phishing emails with links that can infect devices with data-harvesting malware. Sensitive information is bought and sold among criminals on the dark web and via apps, which other criminals then use to better target their victims.

Of the hundreds of fraud types in play, I believe three are of particular concern: the tech support scam, the bank impostor scam, and financial grooming.

Tech Support Scam

A tech support scam may originate with a call from someone claiming to be with Microsoft or Windows tech support, or via a popup window on your device screen. The target is warned that a virus has been detected, and to protect their data, they must go to a web address or call a provided phone number. Inevitably, the "tech support" person convinces the target to allow them to remotely access their device, leading often to even more complexity to the scam and massive financial losses.

Helen, from Southern California, told AARP's Fraud Watch Helpline that she received a pop-up message on her computer screen along with a loud voice warning: "Do not turn off your computer!" Helen was instructed to call the phone number on her screen, and she soon found herself talking to someone who claimed to be a tech support staffer from Microsoft. The fake tech support staffer told her that her computer was under attack and convinced her to download software that gave him access to her computer and its data.

Helen didn't realize that the "helpful" technician was part of a fraud ring, and that the pop up on her computer was a fake. He offered to put her through to the security department, where someone posing as a bank official told her that hackers already were stealing from her account, and she needed to quickly move her funds to a new, safe account. Helen followed his instructions, withdrawing cash and buying gift cards and sending wire transfers and cashier's checks to addresses in other cities. Most of her retirement nest egg was stolen before a bank fraud investigator intervened, convincing her to speak to her family about what was happening.

Bank Impostor Scam

In this growing scam, a target receives a text message from what appears to be their bank, asking them if a certain transaction made on their account is legitimate, typically requesting a Yes or No response. The target sees a transaction they didn't make and responds No.

A phone call immediately follows, ostensibly from their bank. The caller explains that they are their bank's fraud investigator, and their accounts are actively being hacked. The fake bank investigator then helps the target transfer their assets to keep them safe. The ending is always the same; it wasn't the person's actual bank and the victim's assets have been stolen with little chance of recovery.

Magis, who reached out to AARP's Fraud Watch Network Helpline, experienced this scheme. She was made to believe that her bank's fraud investigators were seeking to help her address fraud in her accounts. They told her that her stolen identity was being used by foreign cybercriminals who used it to buy child sexual exploitation materials, murder people, and sell body parts. The impact grew to affect her retirement account, and more than \$1 million was stolen throughout the scam. Magis has suffered significant stress and faces the possibility of being forced to sell her home and face homelessness.

Financial Grooming

Romance scams are sadly common, where a victim is manipulated over time to believe they are in a deep love affair with someone they've met online, only to be crushed when they learn it was all a lie and their savings had been wiped out as well.

A burgeoning form of this scam typically begins with what seems like an errant text message such as, "Hey Bob, are we still on for dinner at 7?" The recipient kindly responds to tell the sender they have the wrong person, and that is all it takes to build out a conversation, that turns into a friendship that becomes a trusted relationship, that leads to a devastating investment fraud that destroys victims emotionally and financially.

In this particular scam, there are victims on both ends of the crime. Southeast Asian organized crime groups lure frontline scammers with fake job offers. Once they arrive, the criminals take their passports and force them to phish for potential scam victims for endless hours a day under threat of violence and even death. This crime is dubbed by the criminals who came up with it, Pig Butchering - where they fatten the victim before slaughter. The term is so loaded with victim blaming that many in this space refer to it instead as financial grooming.

Their targets are groomed over weeks or months and at some point, the scammer explains that they have such a great life with cars and homes and jewelry because of their investments in cryptocurrency - and they can show the target how to trade. The scammer convinces the target to access an online or app-based crypto exchange and encourages small investments at first. The returns entice the target to invest larger amounts and the returns continue to grow. When the victim decides it's time to cash out, they are told they first have to pay thousands in taxes. The victim may even cash out other accounts to pay the taxes, only to find that the entire ordeal was built on a brutal lie.

While these cases typically focus on fake investments in cryptocurrency, sometimes the commodity is precious metals.

Forms of Payment in Fraud

Fraud criminals take advantage of about every money transfer option to steal from victims. They steal credit and debit card information. They convince victims to withdraw thousands of dollars in cash and ship it or wait in their home until one of the gang members stops by to pick it up.

They coerce victims into making money transfers from their bank accounts or wire transfers from a money service business. They take advantage of Peer-to-Peer platforms. As described earlier, they coerce victims into converting cash into cryptocurrency, and they convince them that purchasing gift cards and sharing the

information on the back of the card will solve the urgent financial matter, and, more recently, they convince victims to buy gold bars.

In gold bar schemes, the criminals may convince victims that their financial accounts are under attack and the safest course of action is to liquidate the assets and purchase gold bars to protect their wealth. Criminals like gold bars because they are easy to transfer across state lines, and it's untraceable once sold and melted down. Some experts suggest that older adults are particularly receptive to gold, and its value has risen significantly in the last five years. At last look, gold was valued at just over \$2,600 an ounce.

As unlikely as it may seem that these ploys work, it's important to keep in mind that the criminals are using how our brains function when in a heightened emotional state against us.

Generative Artificial Intelligence Poses a Threat, But Guidance is the Same

For all of the promises generative artificial intelligence (AI) portends, we ignore its potential for harm at our peril. AI is already being leveraged by fraud criminals to turn grammatically challenged emails and texts into perfectly formed and convincing messages. It's being used to animate still images and create videos and websites from whole cloth. We have learned that AI is used to target attacks on communities of color to affect the appropriate dialect to conduct regionally specific phone-based grandparent scams.

Generative AI is like the industrial revolution for fraud criminals. It enables them to make every possible scam far more difficult to discern. As scary as this sounds, we seek to remind consumers that guidance about scams remains the same. Stay in the know on fraud trends and defensive actions you can take so you are better able to avoid engaging with them. A Path Forward

It may seem that we are in a fraud quagmire with little hope of getting out. There is no single solution, but there are roles for each sector of our society that will go a long way to turning the tide on the fraud tsunami.

For individuals, it's taking steps to better protect ourselves and our loved ones from fraud attacks. Such actions include freezing our credit, using a password manager and multifactor authentication, shredding documents, and keeping our device operating systems updated to protect against known vulnerabilities, putting a freeze on credit reports, and not engaging with incoming messages from unknown persons, and share what we know. Each of us should make it a point to talk about the latest we've heard about fraud with our family members and friends. The more we talk about these scams, the better protected we will be.

For educators, it is important that we tell consumers about the signs of the latest scams and their red flags, but what if we are able to come up with something simpler? If we can train our brains on how most scams come at us and what to do when it does, we could probably thwart a lot of crime. Most scams come as a communication out of the blue that gets us immediately into a heightened emotional state and contains urgency. If we could train consumers that this scenario is likely a scam, we can train them how to react. AARP has been working on this concept with input from people around the globe and are hopeful something can be accomplished.

Industry has a critical role to play as well. Financial institutions must continue to innovate on fraud controls and mitigation. Tech companies must build security into the design and manufacture of technology products, so that products come to market secure by design and safe by default.

Industry and law enforcement should champion the success of the new National Elder Fraud Coordination Center (NEFCC), noted earlier. Even with under-reporting, law enforcement is swimming in a sea of elder fraud reports. Scarce resources make it difficult for investigators to link cases. Jurisdictional challenges that come with transnational organized crime investigations limit prosecutions. Developing high-priority, high-impact cases take time, labor, and analysis. A national coordination center like NEFCC, with the leads, the data analysts, and the combined resources of the private and public sector can overcome these obstacles. In addition to the ability to create rich law enforcement investigative packages, incoming data from members could offer opportunities to neutralize known fraud vectors.

Indeed, just last week, in a new commentary piece for Fortune, Nasdaq Chair and CEO Adena Friedman unveiled new research that shows that annual GDP growth in the US would be 0.5% larger without fraud. Friedman says fraudulent acts too often go unnoticed but can be mitigated by better communication between the public and private sector. NEFCC marks an important and imminent means of producing this coordination.

Policymakers have an important role to bring the fight to fraud crime rings, including legislative solutions such as: providing more resources to train state and local law enforcement to investigate fraud crimes; reinstating of the casualty loss

deduction to address the significant tax burden that fraud victims face having to also pay taxes on the assets that were stolen; limiting the damage of fraud involving cryptocurrency ATMs; improving staffing of DOJ's Elder Justice Strike Forces; and enhanced efforts such as the National Elder Fraud Coordination Center to bring the public and private sectors together to build cases for investigation and prosecution.

Conclusion

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

But, together, educators, policymakers, law enforcement and industry can turn the tide against the vicious crime gangs who hold the power right now. Together, we can disrupt their business model, protect millions of consumers, and keep billions of dollars in savings and retirement accounts and in our economy.

We thank this Committee for bringing attention to this important issue and look forward to working with you to turn the tide on fraud criminals.

U.S. SENATE SPECIAL COMMITTEE ON AGING
"FIGHTING FRAUD: HOW SCAMMERS ARE STEALING FROM OLDER ADULTS"
SEPTEMBER 19, 2024
PREPARED WITNESS STATEMENT
Scott Pirrello

Good morning, Chairman Casey, Ranking Member Braun, and other members of the Senate Special Committee on Aging. I appreciate the opportunity to share my testimony with you today.

My name is Scott Pirrello. I am originally from Long Island, New York and I attended Penn State University. However, I am now a career Elder Abuse Prosecutor for the San Diego District Attorney's Office. In 2018, I felt a call to action after an epiphany that despite being the Elder Abuse Prosecutor for our county that I was seeing ZERO elder scam cases come across my desk even though I was contacted by dozens of victims whenever I was out in the community. When I sought out the answer to the question of why I had zero cases, I was shocked to learn that hundreds of reports existed, but once local police determined that the bad guys were far away overseas, the cases were filed away and never submitted to local prosecutors.

I assumed then, like so many, that certainly someone or some agency was in charge of working on these cases, someone was caring about all these untold victims, and someone was working to stop this problem from happening. I was wrong.

Right at this moment, there are thousands of American seniors all throughout the country being scammed - they are grandparents, aunts and uncles, friends and neighbors, veterans, best-selling authors, engineers, retired teachers and police officers. They are living independent and vibrant lives. They still live in their own homes, still drive a car, help out their families, and volunteer in their communities. And this morning as I testify, they are being terrorized by foreign nationals, on the verge of having their lives destroyed and forced into financial ruin.

This morning as each of them logged onto their computers to check in on their grandchildren or to glance at Facebook, a simple popup message appearing to be from Microsoft may have appeared on their computer screen saying that something was wrong with their computer and that they needed to call a given phone number to fix it. This phone number is often spoofed to appear like a number local to the victim. The scammers, often posing as helpful Microsoft support folks, then convince those seniors to accept a download of a remote access software onto their devices, which authorizes a trojan horse to allow the scammers to see inside their computer. Next the scammers begin to instill fear into their victims by telling the victims that their computers have been hacked and their information has been used for some horrific purpose, such as to view child sexual abuse material, or has been involved in some illegal drug cartel activities.

Once the scammers have access to their devices, the scam shifts towards their finances. The fake Microsoft worker tells the victim that their financial accounts have also been hacked and must be secured. The scammer then transfers the call to a "colleague" - another scammer posing as a representative from a bank security department, the United States Department of the Treasury, Federal Trade Commission (FTC), U.S. Marshalls, or any other federal agency.

The fleecing has begun, and the next ask is a test of whether the scammer has the victim hooked or not. The victims are instructed to withdraw a high value of money, like \$30,000 or more, from their bank - or they are told to purchase gold bars worth \$20 to \$40 to \$60,000. Once the victim has the cash or the gold secured, they are instructed to either send cash through Bitcoin ATM machines or to package it up in cardboard boxes and instructed to either ship it across the country, or they are told that a courier posing as a federal agent will be coming to their house to pick up the package. This will continue until the victim runs out of funds, or until someone interferes.

The scenario I just described is not fictional. This narrative is exactly what occurred in our most recent case in San Diego last week. A 94-year-old Air Force Veteran lost \$143,000 in five separate pickups of cash over a two-week period. According to the FBI's most recent Elder Fraud Report, tech support scams were the most prevalent scams perpetrated against older adults.

Hundreds of thousands of victims from all around the country fight through the humiliation and shame these scams cause each year, and summon the courage to report what has happened to them. They will call their banks and then reach out to their local police departments, their local prosecutors offices, to the Federal Bu-

reau of Investigation (FBI), FTC, or to their State's Attorney General's and Consumer Protection Offices, or perhaps they will try to contact the U.S. Department of Justice (DOJ)'s Transnational Elder Fraud Strike Force, a program highly promoted by the Department of Justice as a potential solution to this scam activity. But these victims will all be met with the most regrettable answer: they will be told, "I'm sorry, but there is nothing that we can do."

I am here today speaking on behalf of the MILLIONS of American elder fraud victims in recent years who have been begging their government, local and federal law enforcement, and the banking, technology, and retail industries to help them. Too many very well intended programs are not implemented in a way to truly impact the tsunami of fraud that we are facing each day.

Currently, we are all failing the very people who need us the most: older adults - many of whom can't afford to lose anything, let alone everything. We are failing in our most basic duties to protect those in their golden years who are living off the nest eggs they worked for their entire lives and who are beyond the ability to rejoin the workforce to make the money back. These are lives in ruin.

Another failure of the status quo is the inability to accurately report on Elder Fraud victims and loss amounts. Without a mechanism for centralized reporting and accounting for all reported cases from all available sources along with reasonable estimates for unreported cases, policymakers are not making informed decisions on resource allocation. By all reasonable measures, the actual amount of losses each year attributed to elder scams in this country likely exceeds one hundred billion dollars.

Since 2019, on the backs of a few patriotic former Marines working in our DA's office and the San Diego's FBI office, we have been working to change this narrative and prove that contrary to the strategy of surrender, something COULD be done to fight this siege on older adults. To fight the status quo, we had to develop methods and strategies to at least mount a counterstrike.

In 2021, under the leadership of San Diego County's elected DA, Summer Stephan, our office worked with the San Diego FBI to launch a first of its kind Elder Justice Task Force to combat elder fraud. While it was previously thought that all fraudsters were overseas and out of the reach of law enforcement, we have since learned that scammers abroad depend on very organized networks of money launderers operating here within the United States. There are thousands of criminals within these networks who need to be investigated and prosecuted, yet there is no effort outside of ours in San Diego that is dedicated to focusing on these organizations.

The San Diego FBI Elder Justice Task Force (or, EJTF) brought together partners, including the San Diego County District Attorney's Office, the FBI, Adult Protective Services (APS), the DOJ, and our local U.S. Attorney's Office, all local law enforcement agencies, as well as the San Diego Law Enforcement Coordination Fusion Center ("LECC") to work together in an unprecedented fashion to connect the dots and turn small, local fraud investigations into large scale federal investigations and prosecutions. By eliminating the barrier of financial thresholds, the success of each of our EJTF investigations begins with a single local victim using a traditional investigation strategy. Cases are then built through collaboration and utilization of all local resources from APS and law enforcement, coupled with the FBI's incredible capabilities to extend the reach of our investigations outside of our county and throughout the United States, when necessary. Most of these assets of the EJTF are collocated working out of one physical location in San Diego.

The EJTF is now committed to serving these core functions: 1) investigating criminal organizations committing or facilitating fraud within the United States and holding those perpetrators accountable with both state and federal prosecutions; 2) regardless of whether a criminal investigation or prosecution is occurring, working to recover and return funds lost by elder victims wherever possible, including a new aggressive effort to use federal seizure warrants to recover millions of dollars lost by elder fraud victims; 3) collecting and reporting data on the amount of fraud impacting the County of San Diego broken down by jurisdiction; and 4) educating the community, both public and private sectors, about the current greatest threats.

The San Diego EJTF is the only initiative in the nation that is proactively responding to actual elder fraud cases in real time because we are tracking each report of fraud in our county collected by local law enforcement, FBI's IC3.gov database, and APS. We are talking every day to new victims and learning about the new scams and tactics the scammers are using to hook victims. This constant, real-time review of scam reports enables us to lead other agencies, localities, and states when it comes to identifying new scam trends and understanding how these transnational criminal organizations are functioning.

For instance, we have identified tech scams originating in Indian Call Centers as the greatest current threat to our seniors in San Diego and around the country. These scams are facilitated by money laundering cells, primarily made up of foreign actors, who are dispatched from a regional hub, as couriers, to pick up millions of dollars in scam payments.

In the past two years, the San Diego EJTF has worked to disrupt these networks. We have paired local investigators and APS workers with FBI agents to target these networks and we have had success: we have arrested over a dozen of these couriers. We are now routinely filing state prosecutions on these couriers, which have resulted in several federal indictments, including July's indictment by the US Attorney's Office in San Diego of a money laundering ring responsible for receiving stolen funds from over 2,000 victims totaling \$27 million in elder fraud losses.

Despite these successes, the data is astonishing and shows how much work there is still to be done. In our county, we were shocked to see that the amount of losses doubled from 2022 to 2023, with \$98 million from elder victims lost in 2023. Even more shocking is the reality that despite our progress, we are only able to work on one tenth of one percent of the cases we see.

Investing in education, as well as funding task forces like the EJTF, are critically important components in this fight against scammers. Both must be funded adequately. However, we cannot educate ourselves out of this problem nor can we prosecute our way out of this problem.

The only approach that could truly bend the curve resulting in more victims and losses each year will be a holistic whole of nation strategy, similar to what has been assembled in the United Kingdom and Australia in recent years, to identify every opportunity both upstream and downstream of the scam and work to stop the threats. This approach will ultimately eliminate the scammers' ability to attack our seniors on the technology we depend on, make the fleecing of financial accounts more difficult to accomplish, and provide support to the countless Americans who have reported their cases but have never heard back from a single person.

The cause of fighting Elder Fraud does not have a face. It is too siloed and unorganized. The U.S. Senate Special Committee on Aging should take this opportunity to lead and work with all relevant decisionmakers to urgently ensure that not one more victim falls prey to these scams. Through my work, I have seen that our goal should be loftier than creating programs, accumulating data, and writing reports. We can stop this problem entirely and I'm dedicated to joining the Committee in this fight. Every single one of us can do more for these victims, especially for the vibrant grandmother or grandfather who is going to wake up tomorrow to a popup ad from a scammer on their computer. What will be our answer when that victim calls us for help?

****For reference, I will direct you to a submission for the record prepared by another leading advocate in this cause, Ken Westbrook. Mr. Westbrook retired after 33 years in the CIA and is currently the Chief Executive Officer of the Stop Scams Alliance. The Stop Scams Alliance has highlighted the success of other countries, like the United Kingdom and Australia, at stopping scams at the source, and shown how the United States can model these successes.**

U.S. SENATE SPECIAL COMMITTEE ON AGING
"FIGHTING FRAUD: HOW SCAMMERS ARE STEALING FROM OLDER ADULTS"
SEPTEMBER 19, 2024
PREPARED WITNESS STATEMENT
Susan Whitaker

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 Susan Whitaker. I am an Administrative Assistant for the Executive Director of Lehigh County Aging and Adult Services in Allentown, PA. I have been in my current position for four years. My previous employment was for 45 years at The Morning Call, our local newspaper, and a subsidiary of Tribune Publishing.

I am presenting testimony today because my late husband, Bill, was the victim of a scam. I will also share the steps I took once I knew the scam had happened, and the unavailability of the bank we entrusted with our personal account and the business account.

It was a Tuesday night and when I got home, Bill was more quiet than normal. I thought he was just having an off day. He didn't talk a lot the next few days. Bill suffered from dementia and Alzheimer's, diabetes, congestive heart failure, pulmonary embolisms, neuropathy, and gout. At the time of the scam he was 75. Although Bill had sold his business, Bill Whitaker & Son Construction LLC, to his son, Bill stayed on as the office manager. He took care of ordering materials, making payments, and submitting payroll-all the office responsibilities. As the week went on, Bill seemed to be quieter and not talking about anything; he seemed worried.

On Friday night when I came home from work, he started to tell me what had happened. He told me he received an email from QuickBooks, which was used to manage bookkeeping for the business. The email said that the business account had been charged \$499 for an upgrade. He said he didn't order the upgrade. He contacted what he thought was QuickBooks at that point. This person told Bill that in order for him to refund Bill's money, Bill needed to first pay him \$500 and then "QuickBooks," who was really the scammer, would send it right back to him via another payment platform. He was told not to share this with anyone because then he would not be able to get his money back.

Bill was instructed to install an application on the computer so he could transfer the funds directly into the scammer's checking account. He walked Bill through step by step on what he needed to do to give the scammer online access to install the software. Bill also scanned and sent him a copy of his Social Security card and driver's license. Once everything had been setup, the scammer had Bill set up a Venmo account. Finally, he showed Bill how to transfer the \$500 via Venmo. Because the scammer had access to the computer, as Bill was in the middle of typing the number 500, the scammer took control through the software and added an extra zero to the \$500. Now the transfer was for \$5000. He started yelling at Bill for making the error, when in reality Bill had not made a mistake. He then told Bill, "Look what you've done." He said that now Bill needed to send him \$5000 in order for him to send back the \$5000.

That Friday night when I spoke with Bill, he shared with me that now, in addition to the \$499 initial fraudulent upgrade fee that needed to be refunded to the business account, this individual now owed us money from our personal accounts, due to the numerous Venmo transfers. Bill said that this individual would be calling him back that night at 6pm. The phone rang promptly at 6pm. This time, I answered the phone.

The scammer on the other end of the phone was totally surprised to hear someone other than Bill. I asked him to explain the situation we were in. He walked me through all of the charges and Venmo transactions and I questioned his logic and the process he had put Bill through. At this point, I knew it was a scam, but I asked him to please check with his boss. He said he would call me back, and I told him I would be waiting for his call. At this point, I wasn't even sure how much money had been taken from our personal account and the business account.

While waiting for a call back, I shut down the MAC and booted it back up. I created a new login account and deleted the old information. I found the software, which had been installed, and uninstalled it and changed the settings the scammer had set. I also contacted our bank, Truist, through their customer service department. I wanted to put a hold on both accounts to stop the money from being transferred. Since it was after 6pm, customer service was closed until Monday morning

at 8am. Then I called their fraud phone number. They, too, were closed until Monday morning at 8am. Fortunately, we knew the bank manager at the local branch. Bill called him and asked for his help. He said he would do what he could, but wasn't sure he would be able to get any money back or stop any transfers. There never was a call back from the scammer.

Monday morning, while I was at work, Bill called local law enforcement. They spoke with him, and said they would be in touch with the bank and would work with them. The person Bill spoke with was very kind and patient. During that time, I put a stop on all credit reporting, a hold on all accounts and called the Truist headquarters in North Carolina. I never did get to talk to anyone there.

In the end, the scammer took a total of \$28,000 from us. However, the bank, along with law enforcement, recovered \$8,000 of the money taken from our accounts. Because I acted so quickly, they were able to stop these funds before they were dispersed. Despite this, we still lost a total of \$20,000-\$10,000 from our personal accounts and another \$10,000 from the business account.

This scam was devastating and had a devastating effect on Bill-both financially and emotionally. Because we lost \$20,000, and Bill had a lot of chronic health conditions, Bill began to ration his medications. We just couldn't afford them anymore. Bill also felt responsible and felt he owed it to his son to repay the money. He kept saying he was sorry and that he was so stupid. He asked how could he make such a stupid mistake. I assured him that he was only trying to save the business \$499, and that he didn't do anything wrong. For several days, he was very quiet. After the scam, Bill would not answer the phone unless he knew the phone number and he would not open his email until I reviewed it. In addition to not answering emails or phone calls, Bill started to doubt himself in everything he needed to do. His son no longer allowed him to do any office work and so Bill lost his job. He also lost his sense of self-worth. I was really sad to see this very intelligent and past business owner, become so afraid to read emails and use a phone. It was a huge setback for him, and I think contributed to his worsening health conditions. One thing that I learned is that any event such as this has a devastating effect on the victim regardless of the situation and the scam.

Thank you.

U.S. SENATE SPECIAL COMMITTEE ON AGING
 "FIGHTING FRAUD: HOW SCAMMERS ARE STEALING FROM OLDER ADULTS"
 SEPTEMBER 19, 2024
 PREPARED WITNESS STATEMENT
Nancy Gilmer Moore

I would like to thank Ranking Member Braun, Chairman Casey, the other witnesses, and all in attendance for giving me this opportunity to speak about Medicare fraud and scams that target older adults and people with disabilities.

As the Indiana Senior Medicare Patrol (SMP) program director since 2013, I have learned that one of the biggest crimes affecting older Americans and people with disabilities is Medicare fraud, waste, and abuse. In addition to Medicare's own provider-focused fraud prevention units within the Centers for Medicare & Medicaid Services (CMS), the U.S. Administration for Community Living (ACL) funds and supports the beneficiary-focused Senior Medicare Patrol (SMP) program. With programs in every state, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands, SMP's purpose is to educate beneficiaries, caregivers and professionals on how to prevent, detect and report Medicare fraud. In 2023, ACL's 54 SMP projects had a total of 5,532 active team members who conducted 22,356 group outreach and education events, reaching more than 1.2 million people. In addition, the projects had 270,348 one-on-one interactions with, or on behalf of Medicare beneficiaries.

CMS offers no official estimates of total yearly Medicare fraud, but health care experts estimate improper Medicare payments are approximately \$60 billion per year. The U.S. Department of Health and Human Services' Office of Inspector General's (OIG) most recent annual report on SMP indicated that SMP projects reported more than \$111 million in expected Medicare recoveries in 2023. The majority of these recoveries were the result of a case identified by the Louisiana state SMP project where a nurse practitioner was ultimately found guilty of billing for genetic tests and durable medical equipment that patients did not need and telemedicine visits that never occurred.

Our Indiana SMP uses volunteers and in-kind team members, in partnership with most Area Agencies on Aging, four senior centers and a Center for Independent Living to help us educate people about fraud, errors and abuse in Medicare. Our partners give public presentations, exhibit at health and senior fairs and provide individual counseling across Indiana. We also regularly publish statewide social media updates, share social media resources with our local partners, generate earned television and print media through relationships we cultivate with local investigative reporters, and periodically conduct SMP marketing campaigns.

We also collaborate with organizations through a coalition we founded with the Indiana Secretary of State's Office called the Indiana Council Against Senior Exploitation, or IN-CASE. Members include the Indiana Secretary of State's office, the Indiana Attorney General's office, State Health Insurance Assistance Program (SHIP), the Social Security Administration, the Internal Revenue Service, the Indiana State Police, financial institutions, and many others to conduct joint presentations about Medicare fraud and other financial scams that target older adults. The mission of IN-CASE is to empower Indiana communities to prevent and end senior financial exploitation and other forms of abuse.

SMP programs across the country can provide early detection and warning of emerging frauds and scams. Here are some examples of suspected fraud that the Indiana SMP reported to the OIG during the past year:

- In the Intermittent Urinary Catheter fraud scheme, most of the beneficiaries noticed billing for urinary catheters on their Medicare statements that they and their doctor neither ordered, needed nor received. Many were billed for multiple months with Medicare paying about \$1,500/per month for each separate billing. I personally noticed billings for urinary catheters on my own Medicare statements for May and June and promptly reported the suspicious claims to CMS and requested a new Medicare number since mine was compromised. Beneficiaries may not regularly read or understand their Medicare statements, and therefore may not realize their Medicare number had been compromised. They may also not understand the need to report the fraudulent billing to CMS. Just last week we received a fraud report from a beneficiary who was billed for ostomy supplies she neither received, needs nor ordered. Other SMPs throughout the nation are just now hearing about this fraud scheme as well.

•Another prevalent fraud scheme is genetic testing scams where beneficiaries receive a phone call, email or text advising that Medicare is providing free genetic testing for cancer or heart problems. The caller offers to mail them a cheek-swab kit, and either requests their Medicare number or asks them to confirm it. In one case, the beneficiary contacted Indiana SMP after the scammer called to inform her the swab kit was on her front porch, and they could walk her through the testing and mailing process. The beneficiary got suspicious and fortunately called the IN SMP. As a result, we were able to educate this beneficiary, help her report the scheme, and request a new Medicare number.

•Durable Medical Equipment (DME) fraud is a perennial scam which includes all types of orthotic braces. Beneficiaries continue to contact Indiana SMP reporting unsolicited calls identifying themselves as representing Medicare with an offer of free orthotic braces. The scam often begins with an initial contact from a call center, which makes a referral to an unscrupulous doctor or telemedicine company, and a final referral to a DME provider. The braces delivered are often inferior, and the beneficiary's personal doctor is not typically notified nor consulted. This fraud scheme is another avenue the scammers use to get beneficiaries' Medicare numbers.

•An emerging scam we are seeing throughout the nation is beneficiaries receiving calls allegedly from CVS Pharmacy requesting they order diabetic supplies or medications they do not need. In the cases we have documented in Indiana, the caller already has the beneficiary's Medicare number indicating that the beneficiaries' Medicare number has likely been compromised. Thankfully, none of our Indiana beneficiaries impacted by this have noticed any suspicious charges so far but we have asked them to keep an eye on their notices to ensure no charges pop up. CVS is aware of this scheme and has posted a warning on their website.

The Indiana SMP recommends that all Medicare enrollees and their caregivers review their Medicare Summary Notices (MSNs) for Medicare fee-for-service or Explanation of Benefits (EOBs) for Medicare Advantage plans. Beneficiaries should be on the lookout for duplicate billing, services or products not rendered or received and services not ordered by their physician. We also remind beneficiaries and caregivers that they should never give their Medicare number or financial information over the telephone to an unknown caller, and that Medicare does not make unsolicited phone calls.

Ensuring the financial integrity of Medicare is essential to the millions of Americans who currently depend on it to access comprehensive health care services as well as the thousands of people who become newly eligible for Medicare every day. As US citizens, we all need to become better, more conscientious health care consumers and help identify any potential improper payments. To that end, we have supported Sen. Braun's and this Committee's work to reduce or eliminate Medicare fraud. We assisted Sen. Braun's office with information and language regarding his Medicare Transaction Fraud Prevention Act, which would enhance the Medicare fraud prevention system to alert the beneficiary being scammed.

Thank you for allowing me this opportunity to share my experiences with you today.

Questions for the Record

U.S. SENATE SPECIAL COMMITTEE ON AGING
"FIGHTING FRAUD: HOW SCAMMERS ARE STEALING FROM OLDER ADULTS"
SEPTEMBER 19, 2024
QUESTIONS FOR THE RECORD
Kathy Stokes

Senator Kirsten Gillibrand

Pre-Election Scams

In the leadup to local, state and national elections, phishing attempts generally tend to increase. Scammers will circulate emails, text messages, social media messages, and phone calls pretending to be election authorities, campaigns, or even candidates themselves, in an attempt to deliberately misinform voters, extract sensitive personal information from them, or link them to malicious websites.

Question:

What sort of phishing tactics should older Americans be on the lookout for as they prepare to vote this November?

In what ways can we prevent older Americans from being scammed by these increased phishing attempts that soar every election year?

Response:

Criminals often take advantage of current events to steal money or personal information from people. For example, during tax season, we see an increase in tax and IRS impersonation scams. These can very convincingly mimic the real IRS. At the holidays, as people are buying more gifts, we see an increase in holiday-related scams, such as shopping and gift card scams. Similarly, around elections we may see a variety of election-related scams, such as voter registration scams, AI-generated content designed to mislead voters, donation scams, and fake polls. A search of AARP's scam map shows additional examples of scams in this space: <https://www.aarp.org/money/scams-fraud/tracking-map/>.

While there are many different types of scams, there are similar indicators across all scams. Key indicators of fraud include contact initiated by another party out of the blue and requests for personal information or money, often combined with a sense of urgency designed to make victims overlook signs that the request may not be legitimate. We tell consumers that they must always be on the lookout for scams and verify any information that you receive unsolicited. Our advice to consumers is to never respond to text messages, phone calls, or emails from unknown parties and to go to the purported source of information directly to verify it. AARP's Fraud Watch Network Helpline is a free resource to anyone who has questions about fraud. We speak with people who have been the victim of fraud, know someone who has, or need more information to help them determine whether something is fraud.

U.S. SENATE SPECIAL COMMITTEE ON AGING
 "FIGHTING FRAUD: HOW SCAMMERS ARE STEALING FROM OLDER ADULTS"
 SEPTEMBER 19, 2024
 QUESTIONS FOR THE RECORD
 Scott Pirrello

Senator Kirsten Gillibrand

Financial Security on Digital Payment Apps

Popular digital payment apps, like Venmo, PayPal, and Cash App, are increasingly being used as substitutes for a traditional bank or credit union account, yet they lack the same deposit insurance and protections against fraud that traditional banks and credit cards employ.

Question:

How can we improve consumer safeguards to reduce financial loss among older adults?

To what extent would it be useful to establish standards for these digital payment companies to provide the same protections against fraud that banks and credit cards employ?

Scam Reporting Improvements

Data about the extent to which frauds and scams occur in the United States is imprecise due to the lack of a centralized reporting network and chronic under-reporting.

Question:

How can we improve data collection on frauds and scams, and in what ways would a centralized reporting database assist in better identifying, addressing, and preventing the scams experienced by older Americans on a daily basis?

Response:

It was an honor to be invited to testify last month at the U.S. Senate Special Committee on Aging's hearing on "Fighting Fraud: How Scammers are Stealing from Older Adults" held on September 19, 2024. I was proud to represent the San Diego District Attorney's Office and San Diego's Elder Justice Task Force.

I am following up on your request for written supplemental materials on the topic of holding Bitcoin ATM Machine Companies accountable for the hundreds of millions of dollars in fraud that is being facilitated on their machines. The ideas below are some of the leading ideas being discussed amongst the group of advocates and experts in the area of elder fraud.

Bitcoin ATM Companies can be more accountable and elder fraud victims can be saved from losing their life savings by adopting legislation that could focus on the following areas:

- I. Preventing victims from conducting transactions on these machines at all;
 - a. Consider banning of Bitcoin ATM machines entirely like the UK and Singapore already have (please see attached articles);
 - b. Transaction Limits. California recently enacted Assembly Bill 401 limiting transactions to \$1,000 per day, per customer, and takes effect January 1, 2025. This will have a substantial impact and should be a model for the rest of the country although we are already seeing our scam victims driving from store to store using many machines instead of just one;
 - c. Increase warnings and ensure victims are acknowledging the warnings. ATM companies rely on compliance with "Know Your Customer" (or "KYC") policies as their main safeguard for victims because ATM machine users need to scan their driver's license on the machine before conducting a transaction. ATM machines offer warning screens for consumers but the warnings are oversimplified and ineffective. When the KYC reveals users of advanced age, there could be even additional warnings;
 - d. Enlisting store clerks to help shut down this activity if they take on the responsibility of hosting a machine in their business. Most business locations that operate a Bitcoin ATM machine are convenient stores, liquor stores, and smoke shops. ATM Companies pay these stores a fee to install machines in the stores and

then a monthly stipend to keep them there. Store managers often tell us they see nothing but seniors walking up to these machines and don't know that they need to intervene. If vendors and store clerks were required to complete trainings on spotting and stopping victims, especially elderly people using machines under duress, perhaps paid for by the ATM machine companies, then our store clerks would know questions to ask a senior who appears to be out of place and under duress trying to conduct a transaction at these machines, just like a bank teller would;

II. Slowing down the transactions so that victim's funds can't be converted instantaneously into Bitcoin and transferred across the globe in mere seconds;

a. A holding period or delay of time similar to the wait required for funds to clear after a large bank deposit or wire transfer would significantly impact the ease in which victims are fleeced of their savings using these machines by allowing time for intervention;

III. Creating civil liability causes of action for victims to pursue ATM operators if they do not comply with minimum rules;

a. Creating a cause of action for customers to pursue ATM companies for failing to comply with certain safeguards would create accountability.

Overseas scammers are more frequently using Bitcoin ATM machines as a primary method to get money from elder victims here in California and around the country. According to the attached article published by the FTC just last month, American consumers fed over \$110 MILLION in cash into these machines in 2023 instantly losing their well-earned nest eggs.

Elder victims are routinely coerced to drive to convenient stores, liquor stores, or smoke shops to locate a Bitcoin ATM machine and feed their cash into it. The cash put into the machines is used to purchase Bitcoin converting the cash into a virtual Bitcoin wallet that the scammers overseas can immediately access and liquidate by transferring the funds onto another Bitcoin wallet that is held on a foreign exchange beyond the reach of United States Law Enforcement and legal process.

Because of the nature of these transactions where United States currency is converted to Bitcoin currency, law enforcement's frustration is growing because we cannot seize the cash from these machines even after a fraud is reported and search warrants are obtained. The cash sitting in the machine does not represent the victim's stolen money any longer but rather are the proceeds of a currency conversion transaction and is the legal property of the ATM company at that point. Law enforcement attempting to impound victim's money from these ATM machines risk a civil lawsuit under the theory of conversion and so several reports exist around the country, including our own attempts in San Diego, where victim's money is initially rescued but ultimately has to be returned to the ATM company that facilitated the fraud in the first place.

In addition to the ideas proposed above and the attached Data Spotlight by the FTC, I am also including some additional articles and references to assist the Committee in your consideration. As cited in my oral and written testimony, countries like the UK, Australia, and Singapore are showing how government action and a whole of government strategy can actually bend the curve and actually reduce scam activity.

Thank you again for the opportunity to participate in this critically important dialogue on combatting elder fraud.



For Release

New FTC Data Shows Massive Increase in Losses to Bitcoin ATM Scams

Reports from consumers show nearly tenfold increase since 2020 in amount lost to scammers using Bitcoin ATMs

September 3, 2024



Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Imposter](#) | [Money Transfers](#) | [Consumer Sentinel Network](#) | [deceptive/misleading conduct](#) | [Finance](#) | [Credit and Finance](#) | [Tech](#) | [FinTech](#)

New data [from the Federal Trade Commission](#) shows a massive increase in the amount of money consumers report losing to scammers involving Bitcoin ATM machines. Since 2020, the amount consumers reported losing has increased nearly tenfold to over \$110 million in 2023.

Bitcoin ATMs are machines that look like a traditional ATM and are often found at convenience stores, gas stations and other high-traffic areas. Instead of distributing cash, they accept cash in exchange for cryptocurrency. Their use by scammers, who urge consumers to deposit cash into them to “protect” their savings, is on the rise.

In a newly released data spotlight, the FTC says that fraud losses to Bitcoin ATMs have topped \$65 million in just the first six months of 2024. During this timeframe, consumers over the age of 60 were more than three times as likely as younger adults to report losing money to Bitcoin ATM scams. Across all ages, the median loss reported in the first half of this year was a staggering \$10,000.

The majority of scam losses involving Bitcoin ATMs come as a result of government impersonation, business impersonation, and tech support scams. The lies told by scammers vary, but they all create some urgent justification for consumers to take cash out of their bank accounts and put it into a

Give Feedback

Bitcoin ATM. As soon as consumers scan a QR code provided by scammers at the machine, their cash is deposited straight into the scammers' crypto account.

The spotlight includes tips for consumers to avoid being drawn into scams like these, including:

- Never click on links or respond directly to unexpected calls, messages, or computer pop-ups. If you think it could be legitimate, contact the company or agency, but look up their number or website yourself. Don't use the phone number the caller or message gave you.
- Slow down. Scammers want to rush you, so stop and check it out. Before you do anything else, talk with someone you trust.
- Never withdraw cash in response to an unexpected call or message. Only scammers will tell you to do that.
- Don't believe anyone who says you need to use a Bitcoin ATM, buy gift cards, or move money to protect it or fix a problem. Real businesses and government agencies will never do that – and anyone who asks is a scammer.

The Federal Trade Commission works to promote competition and [protect and educate consumer](#).

The FTC will never demand money, make threats, tell you to transfer money, or promise you a prize.

Learn more about consumer topics at [consumer.ftc.gov](#), or report fraud, scams, and bad business practices at [ReportFraud.ftc.gov](#). Follow the [FTC on social media](#), read [consumer alerts](#) and the [business blog](#), and [sign up to get the latest FTC news and alerts](#).

Give Feedback

Contact Information

Contact for Consumers

FTC Consumer Response Center
[877-382-4357](tel:877-382-4357)
<https://reportfraud.ftc.gov>

Media Contact

[Jay Mayfield](#)
Office of Public Affairs
[202-326-2656](tel:202-326-2656)



Consumer Protection Data Spotlight

FTC reporting back to you

Data Spotlight

Bitcoin ATMs: A payment portal for scammers

By: Emma Fletcher | September 3, 2024 | [f](#) [X](#) [in](#)

Bitcoin ATMs (or BTMs)^[1] have been popping up at convenience stores, gas stations, and other high traffic areas for years.^[2] For some, they're a convenient way to buy or send crypto, but for scammers they've become an easy way to steal. FTC Consumer Sentinel Network data show that fraud losses at BTMs are skyrocketing, increasing nearly tenfold from 2020 to 2023, and topping \$65 million in just the first half of 2024.^[3] Since the vast majority of frauds are not reported, this likely reflects only a fraction of the actual harm.^[4]

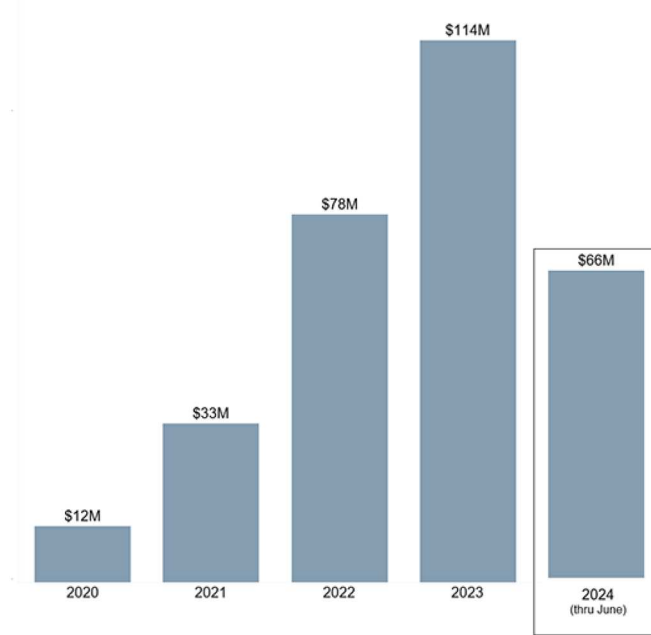
Cryptocurrency surged as a major payment method for scams in recent years, along with the massive growth in crypto payments on fake investment opportunities.^[5] But now crypto is a top payment method for many other scams, too.^[6] Widespread access to BTMs has helped make this possible. Reports of losses using BTMs are overwhelmingly about government impersonation, business impersonation, and tech support scams.^[7] And when people used BTMs, their reported losses are exceptionally high. In the first six months of 2024, the median loss people reported was \$10,000.^[8]

In the first half of the year, people 60 and over were more than three times as likely as younger adults to report a loss using a BTM.^[9] In fact, more than two of every three dollars reported lost to fraud using these machines was lost by an older adult.^[10]

Give Feedback

Reported BTM fraud losses by year

January 2020 - June 2024



These figures are estimates based on keyword analysis of the narratives provided in reports to the FTC's Consumer Sentinel Network that identified cryptocurrency as the payment method. Not all reports identify a payment method or include sufficient details in the report narrative to determine whether a BTM was used. The estimated number of reports by year are as follows: 902 (2020), 1,981 (2021), 3,698 (2022), 4,863 (2023), and 2,968 (through June 2024).

Scams that use BTMs work in lots of different ways. Many start with a call or message about supposed suspicious activity or unauthorized charges on an account. [\[1\]](#) Others get your attention with a fake security warning on your computer, often impersonating a company like Microsoft or Apple. These things

Give Feedback

are hard to ignore, and that's the point. From there, the story quickly escalates. They might say all your money is at risk, or your information has been linked to money laundering or even drug smuggling. The scammer may get a fake government agent on the line – maybe even claiming to be from the "FTC" – to up the ante.

So where do BTMs fit into the story? Scammers claim that depositing cash into these machines will protect your money or fix the fake problem they've concocted. They've even called BTMs "safety

lockers.” They direct you to go to your bank to take out cash. Next, they send you to a nearby ATM location – often a specific one – to deposit the cash you just took out of your bank account.^[12] They text you a QR code to scan at the machine, and once you do, the cash you deposit goes right into the scammer’s wallet.

So how can you spot and steer clear of these scams?

- Never click on links or respond directly to unexpected calls, messages, or computer pop-ups. If you think it could be legit, contact the company or agency, but look up their number or website yourself. Don’t use the one the caller or message gave you.
- Slow down. Scammers want to rush you, so stop and check it out. Before you do anything else, talk with someone you trust.
- Never withdraw cash in response to an unexpected call or message. Only scammers will tell you to do that.
- Don’t believe anyone who says you need to use a Bitcoin ATM, buy gift cards, or move money to protect it or fix a problem. Real businesses and government agencies will never do that – and anyone who asks is a scammer.

To spot and avoid scams visit ftc.gov/scams. Report scams to the FTC at ReportFraud.ftc.gov.

[1] While machines that allow consumers to buy cryptocurrency are commonly referred to as Bitcoin ATMs or BTMs, these machines often handle – and scams can take place in – other cryptocurrencies in addition to Bitcoin.

[2] ATM installations self-reported by operators to an industry website increased from about 4,250 in January 2020 to about 32,000 in June 2024. See trend chart available at <https://coinatradar.com/charts/growth/united-states/>

[3] These and other figures throughout this Spotlight are estimates based on keyword analysis of the narratives provided in reports that identified cryptocurrency as the payment method. Not all reports identify a payment method or include sufficient details in the report narrative to determine whether a ATM was used.

[4] See Anderson, K. B., To Whom Do Victims of Mass-Market Consumer Fraud Complain? at 1 (May 2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3852323 (study showed only 4.8% of people who experienced mass-market consumer fraud complained to a Better Business Bureau or a government entity).

[5] See FTC Consumer Protection Data Spotlight, Reports Show Scammers Cashing in on Crypto Craze (June 3, 2022), available at <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammerscashing-crypto-craze>.

[6] In the first half of 2024, cryptocurrency was the top payment method in terms of aggregate reported losses on tech support scams and job scams, and the second most costly method after bank transfers on business impersonation scams, government

impersonation scams, romance scams, and family and friend impersonation scams.

[7] In the first half of 2024, about 86% of people who reported a fraud loss using a BTM indicated that it was on a government impersonation, business impersonation, and/or tech support scam. This excludes reports categorized as unspecified.

[8] In the first half of 2024, the median individual reported fraud loss when cryptocurrency was the reported payment method (including reports with and without BTM use) was \$5,400; the median individual reported loss to fraud generally was \$447.

[9] This comparison of older and younger consumers' reporting rates is normalized based on the population size of each age group using the Census Bureau's 2018-2022 American Community Survey 5-Year Estimates. This excludes reports that did not include consumer age information.

[10] In the first half of 2024, people 60 and over reported losing \$46 million using BTMs, or about 71% of the reported losses using these machines. During the same period, when a reported cryptocurrency fraud loss did not involve the use of a BTM, about 72% of the losses were reported by people 18 to 59. Most of these losses were to fake cryptocurrency investment opportunities. Percentage calculations exclude reports that did not include consumer age information.

[11] Phone calls were the initial contact method in about 47% of these reports, followed by online ads or pop-ups (16%), and e-mails (9%). Reports indicating online ad or pop-up as the contact method typically described fake computer security alerts. People reported that security pop-ups and email messages included a phone number to call for help.

[12] Reports show that scammers direct people to specific BTM locations and many consumers name the BTM operator in their reports. These details show a pattern that suggests scammers prefer some operators over others and that these preferences have changed over time. While the reports do not tell us why this might be, differences in fraud prevention measures taken by various operators likely play a role.

Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Imposter](#) | [Money Transfers](#) | [Consumer Sentinel Network](#) | [deceptive/misleading conduct](#) | [Finance](#) | [Credit and Finance](#) | [Privacy and Security](#) | [Tech](#) | [FinTech](#)

[Bitcoin ATMs: A payment portal for scammers](#) (317.55 KB)

More from the Data Spotlight

Data Spotlight

[Who's who in scams: a spring roundup](#)

Emma Fletcher | May 24, 2024

Data Spotlight


[Impersonation scams: not what they used to be](#)

April 1, 2024

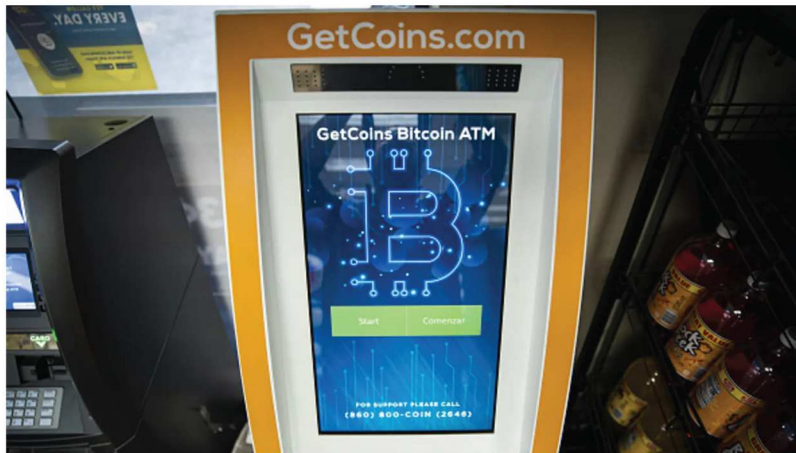
BUSINESS NEWS

Bitcoin ATM scams are soaring — and older adults are increasingly the victims

PUBLISHED SUN, SEP 1 2024 4:03 PM EDT

 **NBC NEWS** | Rob Wile, Christine Romans

WATCH LIVE



A Bitcoin automated teller machine (ATM) at a gas station in Washington, DC, US, on Thursday, Jan. 19, 2023. Bitcoin steadied after snapping a rare 14-day winning streak as a mood of caution supplanted the risk appetite that drove up a variety of assets at the start of the year. Photographer: Al Drago/Bloomberg via Getty Images

Bloomberg | Bloomberg | Getty Images

KELLY EVANS BREAKS DOWN THE INTERSECTION OF WASHINGTON AND WALL STREET

The Exchange Newsletter

SIGN UP



And older people are getting roped in the most. The agency said consumers over age 60 were more than three times as likely as younger adults to say they were duped out of cash in these schemes.

“Scammers are using these machines as a way to take money from people more than we’ve seen in the past,” Emma Fletcher, a senior data researcher at the FTC, told NBC News.

Bitcoin ATMs look like traditional ATMs and operate similarly, in that they can be used for both deposits and withdrawals, but the transactions involve cryptocurrencies.

The machines are banned in some countries, including the U.K. and Singapore, but they’re legal in the U.S. [According to one estimate](#), there are nearly 32,000 nationwide today, up from just over 4,000 at the start of 2020. The kiosks can now be found in high-traffic locations like convenience stores, gas stations and supermarkets — something that has helped fuel the fraud uptick, federal authorities say.

In many of the incidents the FTC identified, fraudsters contact a victim — or the victim inadvertently connects with them — claiming to be a customer service representative flagging an attempted identify theft or an account breach.

FTC warns of increase in crypto ATM fraud scams

01:53



typically directed to scan the code and deposit cash into the Bitcoin ATM, which converts it into bitcoin that immediately gets transferred to the scammer — all while the victim thinks they're protecting their assets.

Scammers have a number of ways to concoct a successful ruse. There are sometimes multiple fraudsters in on a given heist pretending to be employees of a government agency or business, including major tech firms like Microsoft or Apple, according to the FTC.

A scam often begins when bad actors get their hands on a victim's phone number — many of which are increasingly available on the “dark web,” the part of the internet that typical browsers and search engines can't reach, like certain chatrooms, and that has helped enable illegal activity.

Fraudsters will often contact victims claiming to flag an urgent problem with an account, sometimes through a message that looks like a legitimate alert, like a pop-up notification.

“They're trying to create a situation that is really hard to ignore,” Fletcher said. “From there, people are convinced that the problem is actually extremely serious.”

Indiana resident Marilyn LoCascio, 76, says she lost \$31,500 to a fraud group that included people posing as an Apple tech support specialist, a bank representative and two government officials. It began when she received what looked like a security alert on her iPad, which led her to a fraudster who informed her she'd been hacked, with a payment to an online porn website from her account made in her name.

“I just called the number without thinking. ... It would be anything other than Apple,” LoCascio said. “A gentlemen answered the phone who was supposedly a tech, and he even gave me a case ID, and then it just sort of mushroomed from there.”

As her interactions with the scammers dragged on, LoCascio sensed something was wrong. But after being brought into a conference call with someone posing as a U.S. Treasury official, she was persuaded nothing was amiss. She added that she'd never



even heard of Bitcoin, but the apparent urgency of the situation made it seem prudent to follow instructions to protect herself.

Scams involving cryptocurrency have surged alongside the price of Bitcoin, which today is worth about \$60,000, roughly double its value a year ago. But Fletcher said that while many of such frauds, like shady investment schemes, are more likely to victimize younger people, roughly \$2 out of every \$3 lost in a scam involving a bitcoin ATM belonged to someone near or over retirement age.

“These Bitcoin ATMs seem to have opened up sort of a gateway for scammers who are after cryptocurrency to target older adults,” she said.

Bitcoin ATM operators say they have guardrails to fend off fraud and illicit activity.

“We provide numerous scam warnings at our machines in nearly every stage of a consumer transaction to prevent individuals from falling victim to frauds and scams,” Scott Buchanan, the chief operating officer of Bitcoin Depot, said in a statement.

The company, which describes itself as the largest bitcoin ATM provider, said its operations are heavily regulated and involve extensive compliance and consumer protection policies. “We also have live customer support over email, chat, text and phone calls and encourage consumers concerned about a potential scam to contact our customer support team prior to transacting,” Buchanan said.

Bitcoin Depot has not been charged with any crime, though it is currently the subject of [at least one lawsuit from a user](#) who alleges she was victimized by a fraudster at one of its kiosks. The company has denied responsibility.

“Unfortunately, like all financial institutions, we cannot prevent every instance of fraud that occurs using our services,” Buchanan said.

Fletcher said some people have caught on to the scam fast enough to alert the ATM operator and eventually recover their money, but such instances are rare. The best move, she said, is to take a breath and think twice before sending money through a



“It’s natural for people to want to respond rapidly to such a message, but because these scams are so prevalent, it’s really important that people slow down and check it out,” Fletcher said.

TRENDING NOW



0.36 0.17% AVAX 27.91 -2.08% DOT 4.40 -3.08% UNI 7.76 1.05% ARB 0.59 -2.50% AAVE 153.67 -2.93% OP 1.73 -3.31% AT

[HOME](#) < [NEWS](#) < [FINANCE](#)

Singapore to Shut Down Bitcoin ATMs Following Central Bank Guidelines

Two major ATM operators, Daenerys and Deodi, have already pulled their bitcoin machines in compliance with Monetary Authority of Singapore's new guidelines

BY SEBASTIAN SINCLAIR / JANUARY 20, 2022 04:25 AM



Bitcoin ATM inside shopping mall; Source: Shutterstock

[SHARE](#)     

KEY TAKEAWAYS

- **Crypto and bitcoin ATMs in Singapore are closing up shop following guidelines on Monday from the country's central bank**

- **Two major ATM operators have already pulled their machines in compliance with the new rules**

Following new Monetary Authority of Singapore (MAS) guidelines [targeting crypto promotions](#) in the country on Monday, bitcoin ATMs are shutting down as operators are being forced to comply with the new measures.

According to a [report by Reuters](#) on Tuesday, Daenerys & Co., Singapore's largest crypto ATM operator in the city-state said it had shut down its machines following the guidelines, which it said had come as a shock.

NEWSLETTER

Subscribe to Blockworks Daily

Email address

SUBSCRIBE

Daenerys has now closed all five of its crypto ATMs which were placed around shopping centers. Deodi Pte, another crypto ATM operator also announced Monday it had closed its sole machine.

"Pursuant to MAS notice, we regret to inform you that we have to shut down our public bitcoin machine with immediate effect," the Deodi announced [via its website](#).

While Singapore has long been viewed as a hub for crypto entrepreneurship and innovation, the latest moves from the central bank indicate the city-state is attempting to clamp down on activity considered outside the remit of regulators.

"Providing in-person access to digital payment tokens (DPT) ... in public areas through the use of automated teller machines is a form of promotion of DPT services to the public," the central bank said in its guidelines on Monday.

Under existing regulations, those providing services pertaining to crypto must register for a license to operate. Out of the 180 applications MAS has received only five have been approved in principle.

Daenerys and Deodi are among those that have applied and are still waiting for a license to offer their crypto services, according to the report.

The new moves follow a parliamentary hearing [earlier this month](#), in which the city-state's Minister for Communications and Information, S. Iswaran, emphasized a closer focus on the impact that new technologies such as non-fungible tokens (NFTs), decentralized finance (DeFi) and the metaverse will have on citizens.

“The government will seek to balance between promoting economic vitality, preserving social stability and protecting public security in the digital domain,” the minister said.

Start your day with top crypto insights from David Canellis and Katherine Ross. [Subscribe to the Empire newsletter.](#)

Explore the growing intersection between crypto, macroeconomics, policy and finance with Ben Strack, Casey Wagner and Felix Jauvin. [Subscribe to the Forward Guidance newsletter.](#)

Get alpha directly in your inbox with the [OxResearch newsletter](#) — market highlights, charts, degenerate trade ideas, governance updates, and more.

The Lightspeed newsletter is all things Solana, in your inbox, every day. [Subscribe to daily Solana news](#) from Jack Kubinec and Jeff Albus.

TAGS [ATMS](#) [BITCOIN](#) [CRYPTO](#)

[NEWSLETTER](#)

Blockworks Daily

7.76 0.97% ARB 0.59 -2.53% AAVE 153.64 -2.94% OP 173 -3.38% ATOM 4.92 6.19% MKR 1192.57 -3.02% COMP 45.53 -1.9

[HOME](#) < [NEWS](#) < [MARKETS](#) < [POLICY](#)

Bitcoin ATMs Illegal in the UK, Regulator Says

The FCA “warned” crypto ATM operators in the UK to “shut their machines down” or “face enforcement action”

BY MORGAN CHITTUM / MARCH 11, 2022 01:03 PM



Bitcoin ATM | Source: Shutterstock

SHARE     

KEY TAKEAWAYS

- **There are 80 bitcoin ATMs or tellers in the UK, per data from Coin ATM Radar**

- **The FCA said “people should be prepared to lose all their money” if they invest in crypto assets because they are unregulated**

The Financial Conduct Authority (FCA) said on Friday that all crypto ATMs are prohibited from operating in the UK.

The regulator “warned” crypto ATM operators to “shut their machines down” or “face enforcement action,” according to a Friday [statement](#).

NEWSLETTER

Subscribe to Blockworks Daily

Email address

SUBSCRIBE

[Data from Coin ATM Radar](#) shows 80 bitcoin ATMs or tellers operate in the UK, none of which has been approved to offer crypto ATM services.

“We regularly warn consumers that crypto assets are unregulated and high-risk, which means people are very unlikely to have any protection if things go wrong, so people should be prepared to lose all their money if they choose to invest in them,” the FCA said in its announcement.

The news follows UK tax watchdog Her Majesty’s Revenue and Customs’ confiscation [of three NFTs](#) last month in an almost \$2 million fraud probe.

Three people were arrested on suspicion of fraud as a result of the investigation. Suspects used virtual private networks (VPNs), stolen identities, fake addresses and unregistered phones to try to hide illegal activities.

This was the country’s first seizure of a blockchain-based digital collectible.

Nick Sharp, deputy director of economic crime at Her Majesty’s Revenue and Customs, [told the BBC](#) that the authority is “constantly adapting to new technology to ensure [they] keep pace with how criminals and evaders look to conceal their assets.”

The use of bitcoin ATMs has come under increasing scrutiny elsewhere in the world as well. New licensing guidelines from the Monetary Authority of Singapore (MAS) forced ATM operators there [to shut down](#) in January.

Start your day with top crypto insights from David Canellis and Katherine Ross. [Subscribe to the Empire newsletter.](#)

Explore the growing intersection between crypto, macroeconomics, policy and finance with Ben Strack, Casey Wagner and Felix Jauvin. [Subscribe to the Forward Guidance newsletter.](#)

Get alpha directly in your inbox with the [OxResearch newsletter](#) — market highlights, charts, degenerate trade ideas, governance updates, and more.

The Lightspeed newsletter is all things Solana, in your inbox, every day. [Subscribe to daily Solana news](#) from Jack Kubinec and Jeff Albus.

TAGS [ATM](#) [BITCOIN ATM](#) [CRYPTO ATM](#) [FINANCIAL CONDUCT AUTHORITY](#)
[HER MAJESTY'S REVENUE AND CUSTOMS](#) [REGULATION](#)

NEWSLETTER

Blockworks Daily

[SUBSCRIBE](#)

UPCOMING EVENTS

Digital Asset Summit 2025

U.S. SENATE SPECIAL COMMITTEE ON AGING
"FIGHTING FRAUD: HOW SCAMMERS ARE STEALING FROM OLDER ADULTS"
SEPTEMBER 19, 2024
QUESTIONS FOR THE RECORD
Susan Whitaker

Senator Kirsten Gillibrand

Scam Reporting Improvements

Data about the extent to which frauds and scams occur in the United States is imprecise due to the lack of a centralized reporting network and chronic under-reporting.

A consumer fraud survey conducted by the FTC suggests that less than three percent of individuals who experienced a fraud or scam reported it to a government entity.

Question:

Why do you think the vast majority of people do not report experiencing a fraud or scam?

Response:

I think people do not report experiencing fraud or scam because they are embarrassed to tell anyone. They are older and have worked hard for their savings. To have it taken away from them by a stranger is humiliating. They do not want family and friends to make fun of a mistake they made. (I know this from experience. It is a joke to those not effected, but hurtful to the person who experienced the fraud.) Also, for the most part people in general see the good in others. This allows us to trust those we shouldn't trust.

Question:

Did you or your husband have any reservations in reporting the scam he experienced?

Response:

Bill had reservations. He had been told if he tells anyone, he would not get his money back. He also did not want anyone to tell him he had made a mistake. He was embarrassed and humiliated. He did ask me to not tell anyone of the kids. I had no reservations as I knew this would be the only way to stop more money from being taken. The information shared at work and the training provided taught me that reporting the fraud is the only way to catch the scammers, to help to keep it from happening to other people.

Statement for the Record

U.S. SENATE SPECIAL COMMITTEE ON AGING
"FIGHTING FRAUD: HOW SCAMMERS ARE STEALING FROM OLDER ADULTS"
SEPTEMBER 19, 2024
STATEMENT FOR THE RECORD
America's Credit Unions Testimony

On behalf of America's Credit Unions, I am writing regarding the Committee's hearing entitled, "Fighting Fraud: How Scammers are Stealing from Older Adults." America's Credit Unions is the voice of consumers' best option for financial services: credit unions. We advocate for policies that allow the industry to effectively meet the needs of their over 140 million members nationwide.

We thank you for holding this important hearing on how to combat efforts targeting older Americans. Credit unions were pleased to champion the Senior Safe Act and appreciate its passage in 2018, making it easier for credit union employees to step in and protect seniors facing financial exploitation.

Many credit unions have instituted financial education and literacy programs aimed at older Americans and their families to help educate them about methods of fraud and how to detect scams, and credit unions have enhanced their use of AI-driven fraud detection systems and devoted significant resources to training their staff to recognize signs of elder financial abuse, which helps employees intervene to prevent scams from progressing. Many credit unions have adopted the trusted contact system, which allows elder credit union members to designate a trusted individual who can be alerted by the credit union in case of suspicious account activity. Some credit unions partner with third-party organizations, like Carefull, to offer more comprehensive fraud protection services specifically designed to monitor and protect older adults' finances. These are just some of the ways that credit unions, as member-owned institutions, work to protect their members. America's Credit Unions also facilitates credit union engagement with the National Credit Union Administration and the Consumer Financial Protection Bureau's Office of Older Americans to share information on trends in elder financial exploitation and other resources to help credit unions protect their older members.

Credit unions also invest significantly in both security and compliance management systems to prevent unauthorized electronic fund transfers (EFTs) and support faster, innovative payment options for their members. The credit union industry's commitment to relationship banking also gives members confidence that if they have a problem, they can count on their credit union to make every effort to resolve the issue. This emphasis on high touch service means that members will often seek and receive the help of their credit union even when a transaction primarily implicates the services of a third party with which the credit union has no formal, direct relationship. Member interaction with such services, particularly nonbank payment platforms, can complicate error resolution procedures, place strains on a credit union's compliance resources, and magnify exposure to fraud.

These relationships are also important and necessary because credit unions are committed to supporting consumer payment choice. Many credit unions provide their members with peer-to-peer (P2P) payment services as a convenient, value-added service for which they do not charge exorbitant fees. Credit unions are eager to embrace seamless payment technologies, but to compete effectively against large banks and nonbank financial giants with similar service offerings requires a fair regulatory environment. The costs borne by credit unions stemming from payments-related fraud are growing exponentially and cannot be sustained without limit. Expanding the liability for financial institutions for payments-related fraud would put a major strain on credit union resources and their ability to collaborate with payments platforms and expand consumer choice. This is why we strongly oppose S. 4943, the Protecting Consumers from Payment Scams Act, and believe it is not the correct solution to this problem.

As member-owned, not-for-profit financial cooperatives, credit unions exist to provide credit at competitive rates and offer low-cost services that assist their member-owners in meeting their individual financial needs. Credit unions support efforts to stop fraudulent schemes and invest in robust compliance programs to limit this activity, but an expansion of credit unions' liability for the misdeeds of fraudulent actors would have the unintended effect of limiting consumer choice and access to services. Rather than approaches such as S. 4943, we believe that legislative efforts are better directed at steps to prevent fraud before it occurs, educate consumers about fraud and risks associated with unregulated technologies, and create a level

playing field for currently underregulated fintech companies and insured depository institutions.

Finally, we must also flag our concerns with S. 1838, the Credit Card Competition Act, because of the impact it would have on the industry's efforts to fight fraud. Proponents of this bill say that it targets large banks and will not hurt others. They are wrong. The reality is that it will hurt community financial institutions and consumers, and we strongly oppose this legislation. This bill would require financial institutions to allow credit card transactions to be routed via an alternative network. Additionally, the bill contains an explicit requirement that card issuers enable all types of transactions and security protocols, even if a credit union finds that these methods are unnecessary, unaffordable, or unsecure. Each time a network is added or changed to keep up with merchant demands, hundreds of millions of new cards would have to be issued which would expose consumers to identity fraud through mail theft and increase the cost of the payments system.

Any reduction in interchange fees from this legislation would directly affect credit union investment in fraud management systems and processes that are dedicated to reducing fraud risk in the system-forcing credit unions to increase costs to cover these necessary expenses. This would limit consumers' choice when it comes to credit cards and would allow big box retailers to pick which network will process transactions-resulting in the cheapest and least secure networks handling consumers' personal financial information. Critical consumer protections such as fraud protection could disappear by using these third party, less secure networks.

America's Credit Unions appreciates efforts to promote consumer and industry resilience to fraud but urges you to reject these two misguided legislative approaches. Credit unions are committed to fighting fraud, educating seniors, and sharing information necessary to prevent financial crime. Ideally, legislative solutions should aim to prevent fraud before it occurs and should include bolstering the resources of law enforcement, educating consumers about fraud and scam risks, and creating a level playing field between insured depository institutions and underregulated companies.

We thank you for the opportunity to share our thoughts on this important topic.

Sincerely,

/s/

Jim Nussle, CUDE
President & CEO

cc: Members of the Special Committee on Aging

U.S. SENATE SPECIAL COMMITTEE ON AGING
"FIGHTING FRAUD: HOW SCAMMERS ARE STEALING FROM OLDER ADULTS"
SEPTEMBER 19, 2024
STATEMENT FOR THE RECORD
Defense Credit Union Council Testimony

On behalf of America's Defense and Veteran Credit Unions and our almost 40 million members, I am writing to provide our views and comments for the September 19, 2024, Senate Special Committee on Aging hearing titled, Fighting Fraud: How Scammers are Stealing from Older Adults.

The Defense Credit Union Council (DCUC) is committed to ensuring that our Nation's veterans receive the highest level of financial protection and support. As stewards of financial wellbeing for military members and veterans, we are deeply aware of the growing prevalence of scams that disproportionately target these communities. We encourage our members to take proactive steps to safeguard veterans from falling victim to financial fraud and scams.

We need to combat scams targeting veterans through robust education and awareness programs that continuously develop and disseminate educational resources to veterans and their families. This ensures they are informed about the latest scam tactics and how to recognize fraudulent schemes.

Many of DCUC's member credit unions offer a variety of financial tools and services designed specifically to help veterans manage their finances securely. These tools empower veterans to protect themselves from fraud by monitoring their accounts and making informed financial decisions.

As part of our mission, DCUC engages in policy advocacy at both the state and federal levels to strengthen protections for veterans against financial exploitation. We will continue to actively support legislation that promotes stricter penalties for fraud targeting veterans and advocate for the development of stronger consumer protection regulations.

In addition to prevention efforts, our members are focused on ensuring veterans have access to resources for reporting fraud and recovering from its effects. Our credit unions maintain strong fraud reporting systems and offer personalized support for victims of financial scams.

In addition, DCUC fosters collaboration between financial institutions, veteran service organizations, and fraud prevention networks. These partnerships enhance our ability to create comprehensive solutions that address the unique financial challenges faced by veterans.

Thank you for the opportunity to bring these matters to your attention. Should you have any questions or desire additional information, please do not hesitate to contact me.

Sincerely,

/s/
Jason Stverak
Chief Advocacy Officer
DCUC

cc: Senate Special Committee on Aging Members

U.S. SENATE SPECIAL COMMITTEE ON AGING
 "FIGHTING FRAUD: HOW SCAMMERS ARE STEALING FROM OLDER ADULTS"
 SEPTEMBER 19, 2024
 STATEMENT FOR THE RECORD
Stop Scams Alliance Testimony

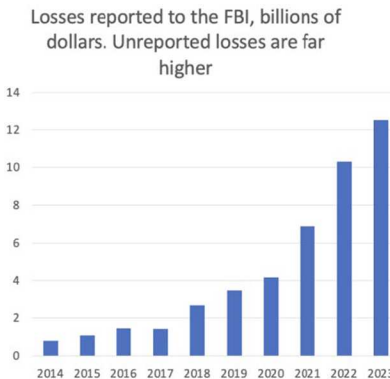
The United States must move rapidly to increase our defenses against a growing national security threat. Criminals—principally based overseas—are using increasingly sophisticated cyber-based techniques to scam Americans at unprecedented levels. A recent Federal Trade Commission report estimates that total U.S. fraud losses might now be as high as \$137.4 billion annually. Losses at this level would exceed annual revenue of such corporations as Verizon, AT&T, or Bank of America. It would also exceed total annual budget of the Department of Homeland Security.

According to a poll conducted by Gallup and the nonprofit Stop Scams Alliance, eight percent of U.S. adults—roughly 21 million Americans—were scammed in the past year. That’s roughly the population of Florida or New York State. In other words, more than 57,000 people are being scammed each day in the United States. That’s 40 victims per minute.

- Scams are Americans’ second-highest crime concern (after the related crime of identity theft), with 57 percent saying they frequently or occasionally worry about it.

- Scams are now among the most common crimes affecting Americans, according to Gallup.

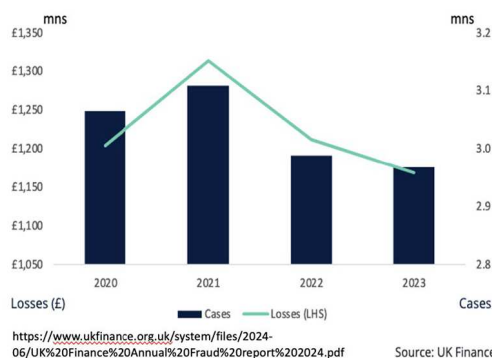
The rate of growth of scams is skyrocketing. According to FBI data, there has been a near 15-fold increase in losses reported to the FBI since 2014; reported losses ballooned 22 percent between 2022 and 2023 alone.



Source: FBI's Internet Crime Complaint Center

Meanwhile, government actions in the UK and Australia are showing signs of progress in the battle against scams. Both countries report double-digit declines in fraud losses in the last year or two. The below chart shows that in the UK, fraud losses and case volumes have declined since 2021, according to the British trade organization UK Finance.

Chart 1 Total fraud losses and case volumes, millions



The below graphic shows the fraud losses reported to the Australian government over the last four years. Australia reports a 13-percent decline between 2022 and 2023.

Combined losses over last 4 years



Why are Australia and the UK making progress in the fight against scams? Both countries have:

- A comprehensive national strategy.
- Someone in charge of implementing the strategy (the Home Secretary in the UK, the Assistant Treasurer and Minister for Financial Services in Australia).
- Annual government surveys to measure the extent of fraud.
- Centralized fraud reporting.
- A national capability to quickly take down fraudulent investment websites.
- Measures to block fraudulent investment advertisements.
- Measures to block spoofed phone calls and text messages.
- Mechanisms for enhanced public-private partnership.
- Nationwide education campaigns.
- New government investment in anti-scam efforts. Each country has found that the investment of a few hundred million dollars can significantly reduce fraud losses.

The United States currently has not taken the above measures. That could change with Congressional action.

Recommendations for Congressional Consideration

It's time to make the fight against foreign organized crime gangs a national priority. We MUST:

1. Create a national strategy to combat consumer fraud

Congress should prioritize the creation of a national anti-scam strategy, as a matter of financial stability and national security. The strategy should establish a national-level task force, clarify authorities about who is in charge in the US Government, and include enhanced public-private partnership involving the tech, telecom, and financial sectors.

Resolution of scam issues is complex and cuts across a number of US agency and Congressional jurisdictions. We need a national strategy that includes a top-down, holistic, across-the-government approach. Congress recently directed US Treasury to do just that:

Financial Fraud.--The Committee is aware that there has been an increase in financial fraud related activity.

Accordingly, the Committee urges the Treasury Department to facilitate a public-private partnership to enhance Americans' financial security and prevent the proliferation of financial fraud and scam schemes. This multisectoral, whole-of-society effort should include the relevant Federal and State financial regulators, consumer protection agencies, law enforcement, financial institutions, trade associations, consumer and privacy advocates, and other stakeholders. This public-private partnership should encourage information sharing among participants, develop best practices for relevant stakeholders, including the larger public, develop educational materials to enhance awareness of financial fraud schemes across sectors, share leading practices and tools, and encourage innovations in counter-fraud technologies, data-analytics, and approaches. The Treasury Department should report to the Committee no later than 1 year after enactment of this act on its progress, including within that report any appropriation or statutory recommendations necessary for achieving this directive. (Financial Services and General Government Appropriations Bill, 2024, S.Rpt. 118-61, July 13, 2023, Cong-Sess:118-1)

The Senate Special Committee on Aging should engage with the Treasury Department to ensure the Committee's views and priorities are taken into account.

Given the severity of the fraud threat, Congress should consider creating a permanent caucus similar to the Senate Caucus on International Narcotics Control. Such a body would help coordinate a holistic response to a complex problem that involves many Committees. Congress could also authorize a Federal Advisory Committee to create a whole-of-government strategy with goals and metrics, drawing on expertise from both the public and private sector experts.

With the proper strategy, we can turn the tide and save millions of victims and tens of billions in losses to the US economy. Other countries like the UK and Australia are showing significant success in the battle against scams by using a holistic approach to stop scams at the source. The US can do the same.

2. Create a formal mechanism for enhanced public-private partnership

The British government is working closely with the private sector, including tech, telecoms and financial institutions. In an "Online Fraud Charter" announced in November 2023, large tech companies volunteered to take nine major steps to reduce fraud on their platforms. If Britain can partner with Google, Microsoft, Facebook, and Amazon to fight scams, so can the United States.

3. Measure the problem

Good public policy requires good data. Congress should direct the Census Bureau to add scams to the biannual National Crime Victimization Survey so we can accurately count victims and losses, and determine the most common threat vectors. The last fraud survey conducted by the Justice Department/Bureau of Justice Statistics (BJS) was in 2017. Congress must provide the funds for annual fraud surveys, which is how the UK and Australia collect the appropriate data to craft their anti-scam strategies.

GAO should combine the siloed information on scams collected by the US government and create the first-ever national estimate of consumer fraud losses. GAO should also recommend ways to improve information collection and sharing across the government.

4. Centralize reporting and enhance information sharing

Centralization and information sharing across government and the private sector will help us identify the threats and respond. Nine nations around the world now have national anti-scam centers-why not the United States?

-A central clearinghouse similar to the National Center for Missing and Exploited Children could efficiently collect the appropriate data, enable quicker action to help victims, and serve as a one-stop shop for educating the public.

-The PATRIOT Act Section 314(b) must be expanded to allow safe-harbor sharing of fraud-related information at scale across industries, including the tech, social media, and telecommunications sectors. (Section 314(b) currently applies only to financial institutions.)

5. A national capability to quickly take down fraudulent investment websites

Centralized data collection, plus expanded authorities for law enforcement, would allow the US to quickly take down fake investment websites, which has proven to be a very effective way to reduce fraud losses due to investment scams. The US gov-

ernment currently takes down some malicious websites, but our process is cumbersome and ad hoc. Meanwhile,

-The Australian Securities and Investment Commission (ASIC) has coordinated the removal of more than 7,300 phishing and investment scam websites since July 2023. The result: Investment scam losses decreased by 29 percent in the second half of 2023. (In the United States, the latest FBI/IC3 report says: "Losses to investment scams rose from \$3.31 billion in 2022 to \$4.57 billion in 2023—a 38% increase.")

-In the UK, most website takedowns are done by the National Cyber Security Centre, an arm of GCHQ (equivalent to our National Security Agency). UK organizations and citizens send 20,000 reports a day of suspicious emails and URLs. The result: 235,000 malicious URLs have been removed since April 2020. Malicious URLs are removed in less than six hours on average, and the median uptime for a cryptocurrency scam website is one hour, according to NCSC. As a result, the number of cryptocurrency scam websites found by the UK government has decreased dramatically since 2021.

UK: Taking Down Cryptocurrency Scams

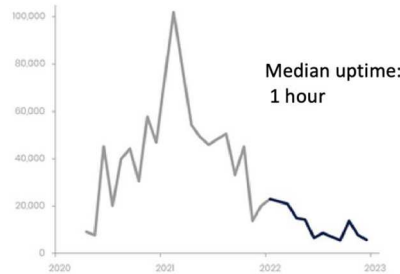


Figure 1: Number of takedowns against cryptocurrency investment scams
<https://www.ncsc.gov.uk/files/ACD6-full-report.pdf>

6. Reduce fake advertising via improved verification procedures

Criminals use fake advertising to entice victims to engage in fraudulent investments. The US should respond by adopting common-sense measures to ensure that financial ads can only be placed by legitimate businesses.

-In the UK, Google says it has seen a "pronounced decline in reports of ads promoting financial scams" since 2021. That's when Google began requiring financial services advertisers to demonstrate that they are on a British government authorized list. In 2022, Google announced that it was expanding its fraudulent ads policy to Australia, Singapore, and Taiwan.

-Meta announced in 2024 that in the UK, financial ads must be authorized by the UK's Financial Conduct Authority before the ad is permitted on Meta's platforms. A similar policy is in place in Taiwan as of 1 August 2024. Meta's policy includes: insurance products, mortgages, loans, investment products and opportunities, and credit card applications.

7. Measures to block spoofed phone calls and text messages

Congress should direct the Federal Communications Commission (FCC) to recommend ways to reduce the ability of criminals to pretend to be legitimate US companies. For example, 12 countries—including the UK and Australia—block inbound international phone calls that spoof domestic numbers. (Example: A call from India that pretends to be calling from Los Angeles.) Because most scams emanate from foreign criminals, this measure has achieved significant results. Spain has announced that it will soon become the 13th country to adopt this common-sense control, which has been proven to be an effective tool in the fight against scams.

The Truth in Caller Act of 2009 is antiquated and needs to be revised to keep up with the increased threat environment.

-The Act currently allows spoofing, as long as the spoofing is not done for fraudulent purposes, but it is very difficult for regulators to determine intent, so the Act is rarely enforced. A better approach would be to define certain calls as illegal, regardless of intent. Example: calls that use a spoofed area code or impersonate a business or government agency. (According to the FTC, "Scams that impersonate

well-known businesses and government agencies are consistently among the top frauds reported to the FTC.”)

-In addition, the penalties in the 2009 Act have eroded with inflation, so they should be increased to deter scammers who pretend they are representing reputable companies.

8. Boost law enforcement resources and intelligence priorities

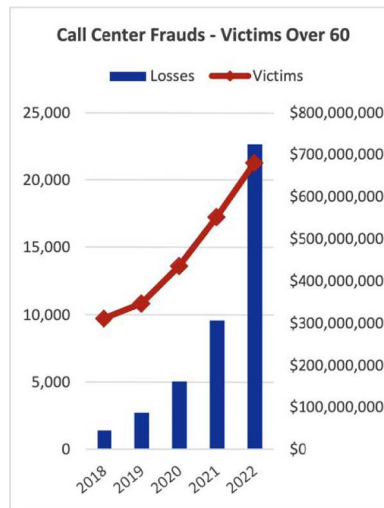
The UK is adding 400 new investigators and ordering their intelligence community to “relentlessly pursue fraudsters wherever they are in the world.” In the US, because of resource constraints, less than 1/10th of 1 percent of fraud cases are investigated, according to a report from the Senate Committee on Aging. A recent study by Syracuse University shows that prosecutions of white-collar crime are down 30 percent from levels reported in 2019. US law enforcement clearly lacks the resources to keep up with the skyrocketing growth of scams. Congress must bolster funding for investigators and provide adequate funds to improve scam training for law enforcement personnel.

9. Mount a focused government-industry effort to combat the “tech support scam”

Measured by the number of victims, the “tech support scam” is the number one scam affecting Americans over the age of 60-by far. The FBI says that this scam has more than double the number of victims than any other scam they measure. The FBI’s IC3 report says:

Call centers overwhelmingly target older adults, to devastating effect. Complainants over the age of 60 lost more to these scams than all other age groups combined, and reportedly remortgaged/foreclosed homes, emptied retirement accounts, and borrowed from family and friends to cover losses in these scams. Some incidents have resulted in suicide because of shame or loss of sustainable income. Tech/Customer Support and Government Impersonation are responsible for over \$1.3 billion in losses.

(Total losses, including unreported, are far higher-perhaps exceeding \$10 billion.)Losses due to tech support/call center fraud are skyrocketing-up more than 14-fold since 2018.



This scam often begins with a “pop-up” that takes over a person’s computer. Criminals pose as technology support representatives and often gain remote access to victims’ devices with software that persists for the life of computer, which enables revictimization.

The Committee should request that the Department of Homeland Security consult with industry partners and deliver a plan to significantly reduce the threat of the tech support scam. The scam begins with malicious software that can be detected or blocked. The report should also include recommendations for reducing the risk imposed by remote access software that can be installed with or without a person’s knowledge and runs without warnings--forever.

The good news is that we can turn the tide. The UK and Australian governments have shown that with an organized and adequately-funded approach, the United States would quickly save millions of victims and tens of billions in losses to the US economy.

U.S. SENATE SPECIAL COMMITTEE ON AGING
 "FIGHTING FRAUD: HOW SCAMMERS ARE STEALING FROM OLDER ADULTS"
 SEPTEMBER 19, 2024
 STATEMENT FOR THE RECORD
Dr. Stacey Wood Testimony

Introduction:

Thank you to Chairman Casey and Ranking Member Braun and the Special Committee on Aging for the opportunity to provide this written testimony.

I am a board certified, licensed clinical psychologist (CA PSY 16805) and hold an endowed chair, the Molly Mason Jones Professor of Psychology at Scripps College. I received a B.A. in Bio-Psychology from Middlebury College, and a PhD in Clinical Neuropsychology from the University of Houston.

My area of research broadly is decision making in older adults with specific application to scam susceptibility across the lifespan. I am a member of the National Institute of Justice's study section panel on financial elder abuse. Furthermore, I have written over 80 publications including books, articles, and chapters related to my research on decision making abilities across the lifespan, undue influence and capacity. My lab's research currently has two major areas of focus at present: (1) scam susceptibility, and (2) the non-economic and emotional impact of fraud victimization on consumers.

I am an active member of the Riverside County Elder Abuse Forensic Center (EAFC) and San Bernardino's Adult Protective Services (APS) in California. In these roles, I conduct interviews and assessments out in the field with older fraud victims, draft reports for the EAFC and APS, and when needed testify in court. I frequently serve as a court appointed Evidence Code section 730 expert for the courts in Southern California on issues related to capacity, undue influence, conservatorships, fraud and financial elder exploitation. I have qualified as an expert in over 50 court proceedings including those in state and federal jurisdictions, civil and criminal proceedings, as well as FINRA hearings.

Susceptibility to Lottery Type Scam Solicitations:

About 10 years ago, I started to become interested in why older adults were complying with lottery sweepstakes type scams which at least to me appeared to be obviously "scammy". Many experiments later, we have learned that all consumers can be susceptible to these types of scams, although there are particular risks for older adults.

Even today based on 2023 Federal Trade Commission data, lottery and sweepstakes scams are the third most commonly reported scams. These scams have high compliance rates of around 15%, and losses average \$800.00. These scams result in \$210.9 million dollars in annual losses. Moving to individuals over 80, sweepstakes / lottery scams are the fourth most common scam but the median loss in this population is \$5,500.¹ In our lab data, we see high compliance rates, closer to 25% with our simulated studies with the following factors increasing risk of compliance: (1) low education, (2) overconfidence, and (3) Bullshxt Receptivity² (rating statements like, "Hidden meaning transforms unparalleled abstract beauty" as profound). Other groups have noted depression, a negative life event, and lower housing wealth as factors³. However, the most potent predictor in our lab-based studies of compliance has been the consumers' in the moment risk assessment where they are asked to estimate the risks and benefits of the solicitations offers. Consumers are overconfident in their ability to detect risk and minimize potential threats while focusing on possible rewards in the moment. These findings echo others' work on the role of emotional arousal and decision-making that increases scam compliance.⁴

As the Committee may note, none of these factors is necessarily overrepresented in older adults. A good question is why do older adults lose so much more money / victimization. We suspect it relates to scammers' higher efforts to target older adults, higher net worth of older adults' accumulated wealth, and some increase in compliance once a scammer has developed a relationship with the victim. We believe

¹ <https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports><https://www.theguardian.com/money/2023/jun/12/older-people-hired-as-money-mules-by-gangs-as-cost-of-living-crisis-bites>

² Add citation for WHY comply, also our JEP article on scams and compliance.

³ Add Deliema 2018, Anderson 2013.

⁴ Add Kircanski-<https://scholar.google.com/citations?view=op=view-citation&hl=en&user=vRVx7dgAAAAJ&citation—for—view=vRVx7dgAAAAJ:i2xiXl-Tujoc>

that increased education informing consumers that foreign lotteries are illegal and structural protections (flagging suspicious bank transfers, temporary holds on funds) are needed to address this persistent and damaging scam.

Non-Economic and Emotional Impact of Scams on Victims:

Recent research on the emotional impact of financial fraud has consistently found that the victim's perception of the emotional impact of fraud victimization is usually more severe than the victim's perception of the financial losses across fraud types.^{5,6} Victims may also report feelings of anger, distrust and betrayal.⁷ This is particularly true when scammers use the names of trusted institutions such as a well-respected national company, like Microsoft as is common in tech scams as part of the pitch to the senior.

Victims who are confused about the details of fraud are far more likely to report non-financial costs such as stress and health problems as a result.⁸ This is often the case as scammers will try to confuse victims, implicating multiple companies or banking institutions in the pitches.

Financial fraud victimization has been linked to poor health, poor sleep and poor quality of life.⁹ Common symptoms after a financial setback are stress, anxiety, worry, rumination, and lack of sleep.^{10,11,12} There is some indication that when funds are restored, stress decreases and health may improve.

Feeling foolish, humiliation, embarrassment, and self-blame result in secondary victimization among fraud victims and decreases their willingness to report fraud. Secondary victimization, resulted from self-blaming, impacts subsequent decision-making and shakes confidence.¹³ These events ultimately cause a decrease in confidence in consumers' general financial decision making who feel that they can't trust themselves and fear making another mistake. I have had several victims say something like, "I can't make another mistake" and choose to do nothing with their remaining funds and push away helpful others.

There are also additional non-economic aspects of victimization, including the time and hassle it can take to report and address the issues and additional expenses. As we can probably all relate, it takes time to report fraudulent charges and monitor that funds have been returned. Elder fraud victims have also reported to me their distress at decimated FICO scores that were built up over a lifetime of prudent behavior. Because scammers may coach victims to tap retirement funds, there can be severe tax implications resulting not only in a devastating loss, but also debt with additional taxes due to the IRS.

Older adults in particular are vulnerable to these impacts as they often live on a fixed income and cannot recover financially in the same way that a younger adult can recover from financial setbacks leading to overall reduced quality of life. It is not realistic for many older adults to return to work to make up for the lost funds. Because of the decreased time horizon for older adults (less time to recover), financial exploitation can have a larger impact on seniors and result in increased worry and fear of living in diminished circumstances as an elderly person. These circumstances can tap into deep seated fears of older adults who grew up during the depression and lived frugally and worked hard to avoid poverty in late life only to face a devastating financial loss later in life.

⁵ Modic, D. & Anderson, R. (2015). Its all over but the crying: The emotional and financial impact of internet fraud. IEEE Security & Privacy September / October 2015.

⁶ European Commission, January 2020. Survey on "Scams and Fraud Experienced by Consumers". <https://ec.europa.eu/info/sites/default/files/aid-development-cooperation-fundamental-rights/ensuring-aid-effectiveness/documents/survey-on-scams-and-fraud-experienced-by-consumers-final-report.pdf>

⁷ Spalek, B. (1999). Exploring the impact of financial crime: A study looking into the effects of the Maxwell Pensioners. *Int R Victimology*, 1999, Vol. 6 pp 213 - 230.

⁸ FINRA (2015). Non-Traditional Costs of Financial Fraud.

⁹ Zunzunegui, M.V. (2017). Financial Fraud and Health: The Case of Spain. *GAc Sanit.* 2017; (31(4)) 313-319.

¹⁰ Button, Lewis & Tapley (2014). Not A Victimless Crime: The Impact of fraud on individual victims and their families. *Security Journal*, 27(1), 36-54.

¹¹ Freshman, A. (2012). Financial Disaster as a Risk factor for Post-traumatic stress disorder: Internet survey of Trauma in Victim of the Madoff Ponzi Scheme. *Health & Social Work.* 2012 FEB; 37 (1): 39-48 DOI 10.1093/hsw/lr002.

¹² Ganzini L., McFarland, B. & Bloom, J.D. (1990). Victims of Fraud: Comparing Victims of White Collar and Violent Crimes. *Bull Am J Psychiatry Law*, Vol. 18, No.1. pp 55 - 63.

¹³ Modic, D. & Anderson, R. (2015). Its all over but the crying: The emotional and financial impact of internet fraud. IEEE Security & Privacy September / October 2015.

Acknowledgements

I would like to thank my collaborators, Yaniv Hanoch, Marian Liu, and David Hengerer for their contributions to this program of research as well as the many undergraduate lab members at the Wood Neuropsychology of Decision-Making Lab of Scripps College. I also want to acknowledge the work of the Riverside County Elder Abuse Forensic Center and San Bernardino Aging and Adult Services for their leadership in the community on this issue.

○