S. HRG. 117–507

STOPPING SENIOR SCAMS: EMPOWERING COMMUNITIES TO FIGHT FRAUD

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING

UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

WASHINGTON, DC

SEPTEMBER 22, 2022

Serial No. 117–23

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
49–819 PDF WASHINGTON : 2023

SPECIAL COMMITTEE ON AGING

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

KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
ELIZABETH WARREN, Massachusetts
JACKY ROSEN, Nevada
MARK KELLY, Arizona
RAPHAEL WARNOCK, Georgia

TIM SCOTT, South Carolina
SUSAN M. COLLINS, Maine
RICHARD BURR, North Carolina
MARCO RUBIO, Florida
MIKE BRAUN, Indiana
RICK SCOTT, Florida
MIKE LEE, Utah

STACY SANDERS, *Majority Staff Director*
NERI MARTINEZ, *Minority Staff Director*

C O N T E N T S

STOPPING SENIOR SCAMS: EMPOWERING COMMUNITIES TO FIGHT FRAUD

THURSDAY, SEPTEMBER 22, 2022

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

The Committee met, pursuant to notice, at 10:03 a.m., via Webex and Room 562, Dirksen Senate Office Building, Hon. Robert P. Casey, Jr., Chairman of the Committee, presiding.

Present: Senators Casey, Gillibrand, Blumenthal, Rosen, Warnock, Tim Scott, Collins, Braun, and Rick Scott.

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

The CHAIRMAN. The hearing will come to order.

We convene today to discuss a topic of the utmost importance to the Aging Committee: fighting frauds and scams targeting seniors. While these predatory schemes have existed for decades, we know that the pandemic has only exacerbated this issue, as fraudsters preyed on fear and uncertainty surrounding the virus. Federal agencies, State governments, and advocates all warn of con artists who will do among the following: they will pose as Federal and State agencies to steal benefits; they will falsify romantic relationships to gain a senior's trust; and by way of a third example, peddle fake health insurance and cures for the virus. Scammers are also using new payment methods, making losses difficult to trace.

The Federal Trade Commission reports that gift cards are the main payment method used by scammers to request and steal money from older adults. In 2021, 27 percent of adults 60 and older who lost money paid a scammer using a gift card or a reloadable card. Peer-to-peer payment apps, like Zelle, Venmo, CashApp, and PayPal, are also increasingly used by scammers.

Today Aurelia Costigan from Pittsburgh, Pennsylvania, will share her experience with a peer-to-peer payment scam. Ms. Costigan's story is all too common. Scammers' requests of payments from seniors by way of these apps have increased exponentially, from two percent in 2017 to ten percent in 2021. That is why I recently led a letter to the Consumer Financial Protection Bureau urging the agency to move forward with guidance, guidance to protect older adults from con artists using these apps. I would like to thank the members of the Committee who joined the letter: Senator Blumenthal, Senator Warren, and Senator Gillibrand. Strong guidance and enforcement are critical, as is education on pre-

venting and responding to these scams. I am also proud that my Stop Senior Scams Act was signed into law in March of this year.

Thanks to Senator Moran, Senator Kelly, and Ranking Member Scott for working alongside me and others to pass this important legislation. Thank you, Ranking Member Scott, for that work. This law creates a Senior Scams Advisory Council to ensure that banks and other businesses have both the information and the tools that they need to train employees to identify and respond to scams. We are grateful to the Federal Trade Commission for its work to lead this effort and pleased that this new Council will hold its first convening one week from today.

Finally, Ranking Member Scott and I are releasing our 2022 Fraud Book. Here is it, and I will hold up both versions in English and in Spanish. We are releasing this; as many of you know, we have done this on an annual basis, but this is the 2022 book, which arms older adults with the information that they need to protect themselves from scammers. This new and improved Fraud Book is available today in both English and in Spanish. The Fraud Book highlights the ten most common scams reported to the Committee's Fraud Hotline, which is staffed Monday through Friday 9 a.m. to 5 p.m. Eastern Time. Seniors and their loved ones can seek assistance with reporting fraud and getting connected to resources. The Fraud Hotline's toll-free number is 1–855–303–9470.

I will read that again. 1–855–303–9470.

I am proud of the Committee's bipartisan leadership on this issue, but we know that we have a lot more work to do. We have a sacred duty to protect seniors and their families against these scammers, these criminals. I look forward to continuing to work together on this, and I will now turn to Ranking Member Scott for his opening statement.

OPENING STATEMENT OF SENATOR TIM SCOTT, RANKING MEMBER

Senator SCOTT. Thank you, Chairman Casey. Thank you for working in a bipartisan fashion on so many of the issues that impact our seniors across the country. The one thing about this Committee that I think all Americans can celebrate is the fact that this is a bipartisan effort to protect our seniors every step of the way, and we need more bipartisanship in Congress without any question, but I thank you for your leadership.

I do think it is important to once again reinforce the hotline. This is the 10th anniversary of the Aging Committee's Fraud Hotline. The number, again, as Chairman Casey has said a couple of times, is 855–303–9470.

It is so important for our seniors to know that there is help out there, and one of the easiest ways for our seniors to find that help is to call the hotline when necessary.

Seniors often live alone or are isolated. Loved ones and vulnerable people are not there for them. I would say that when you think about the scams, the devastating effect it has on people with fixed incomes is undeniable, and it is really hard to replace income when you are on a fixed income.

On average, seniors lose about $34,200 for every instance of a scam or fraud. In 2021, according to the FTC, scammers stole $1

billion from our seniors. A billion dollars. In 2021 alone, in South Carolina, South Carolinians lost $48.4 million to scams and frauds. The consequences to the scams and fraudsters are many for our seniors, including losing purchasing power, trying to maintain good credit, affording the cost of their homes, losing sleep. It is an absolute catastrophic experience when one experiences a scam or fraud.

Scams also have unseen consequences, leaving seniors depressed, embarrassed, and feeling betrayed. For example, Jo Saxton, a Navy veteran from Darlington, South Carolina, last year, she received a call from two scammers impersonating law enforcement. They told her that several people in Texas had stolen her Social Security number and opened up checking accounts, and in order for her to avoid the ramifications of law enforcement, she had to send them $22,000 in cash.

Remember that this all happened over a single day. The sense of urgency and the pressure placed on these seniors to make fast decisions that have financial consequences that are devastating happen so quickly. Under this immense pressure, Jo sent two packages of cash, one to Baltimore, Maryland, the other to Little Rock, Arkansas. These people made her feel as though she had no other choice.

The scam not only put Jo in tremendous financial loss, but also caused her to withdraw from family and friends. Although frauds like the ones we will discuss today are so common, each survivor's story is unique on how it affects their lives.

As the Chairman said, we have our 2022 bipartisan Fraud Book, both in Spanish and English, detailing common scams and how to fight back. Identity theft was the second most reported fraud to the Committee's Fraud Hotline. Further, this year's Fraud Book provides critical information and tips on how to protect yourself. According to the FTC, identify theft was the number one scam in South Carolina in 2021, with 17,642 cases. One in four identity theft victims report experiencing sleep problems, increased anxiety, depression, and anger even six months after the crime.

Scammers are not slowing down. Since 2002, we have seen a 1,600-percent increase in reported scams. A 1,600-percent increase in reported scams. Unbelievable. In 2020, FTC reported 4.9 million scams, and in 2021, that number was 5.7 million, an 18-percent increase in the number. I am thrilled that the Council established by this act that Chairman Casey spoke about earlier, the Stop Seniors Scams Act, helps our seniors, and next week, we will see the first hearing. I look forward to hearing from our witnesses today.

Thank you, Mr. Chairman. I yield back.

The CHAIRMAN. Thank you, Ranking Member Scott.

Before I move to the introductions of our witnesses, I want to acknowledge the members who are here already. Senator Collins, the former Chair of this Committee, has been part of the effort of producing and publicizing Fraud Books in the past. We are grateful for her leadership.

Senator Blumenthal is here from the State of Connecticut as well as Senator Scott from Florida.

Let me move to our witnesses. Our first witness is Dr. Marti DeLiema. Dr. DeLiema is an assistant professor at the University of Minnesota School of Social Work. She is an interdisciplinary ger-

ontologist with a specialization in financial victimization through frauds and scams. Dr. DeLiema has collaborated with a variety of financial institutions, aging organizations, and Federal agencies like the Federal Trade Commission. Doctor, welcome.

Our second witness is Nancy Pham-Klingler. Nancy is a senior adult protective services specialist for San Diego County in California. She has dedicated her career to advocating for older adults, safeguarding their finances, and ensuring their safety. In 2021, she received the Chief Investigator's Commendation Award from the San Diego District Attorney's Bureau of Investigations for her efforts in recovering $75,000 for a senior in her community.

Our third witness is a Pennsylvanian, Aurelia Costigan, born and raised in Pittsburgh, Pennsylvania, which is in Allegheny County. Formerly a school bus driver and health care worker, Ms. Costigan is now retired. She has two daughters, three grandchildren, and two great-grandchildren. She will share her experience today with a scammer who impersonated her bank and the steps she took to respond to the scam. Aurelia, we are grateful you are with us.

Now I will turn to Ranking Member Scott to introduce our fourth and final witness.

Senator SCOTT. Thank you, Mr. Chairman. It is my pleasure to introduce a fellow South Carolinian, Mrs. Polly Fehler. It is my pleasure to talk about Mrs. Fehler. She has resided in Seneca, South Carolina, for the last 32 years. She is a retired nurse, holding a master's in nursing, and a veteran of the Air Force. Thank you for your service, ma'am. She is also a member of St. Mark's United Methodist Church, serving her community as a vessel of God's love. Her most important job, however, is being a loving grandmother to five grandkids ranging from the ages of five to twenty-six years old. I hear being a grandmother is better than being a mother. I hear that rumor all the time. Your son Tim says, "I am not sure that is completely true."

Anyways, in April 2021, scammers conned their way into Mrs. Fehler's computer and online banking, which resulted in the loss of $20,000. This crime hit Mrs. Fehler particularly hard, both financially and emotionally. Mrs. Fehler's testimony today is about her personal experience being a survivor of these scams.

I want to thank you, ma'am, for being willing to share your story. It does take courage to step forward into the light and to help other folks avoid situations like the one you found yourself in, and I am so proud that you are willing to help other folks through your story.

Thank you so much for your willingness to be here today and God bless you.

The CHAIRMAN. Thank you, Ranking Member Scott. Well said in introducing one of our witnesses.

We will begin our testimony now with Dr. DeLiema.

You may begin.

STATEMENT OF MARTI DELIEMA, PH.D., ASSISTANT PROFESSOR, UNIVERSITY OF MINNESOTA SCHOOL OF SOCIAL WORK, ST. PAUL, MINNESOTA

Dr. DELIEMA. Good morning. Thank you, Chairman Casey, Ranking Member Scott, and members of the Committee. My name is Dr. Marti DeLiema, and I am an assistant professor at the University of Minnesota School of Social Work. I conduct research on consumer fraud and strategies to safeguard Americans' financial security.

You invited me today to describe current trends in consumer scams affecting older adults. We can use consumer complaint data compiled by the Federal Trade Commission to explore these trends.

Government imposter scams have been in the top five most reported categories of fraud affecting older adults for multiple years in a row, but the Government agency being impersonated has changed over time: the IRS, SSA, FBI, CMS, and so on. The challenge is to predict which agency's clothes the perpetrators are going to try on next, and to create consumer education campaigns that are robust to these changes.

Throughout the pandemic, business impersonation scams grew exponentially, particularly retail company imposters, but it is romance scams that lead the pack in terms of personal financial costs. In a study I conducted with the FTC, we found that the median reported losses for consumers in their 70's and 80's were $10,000, quadruple the losses reported by young adults.

We can also use reporting data to look at methods of money transfer. Today bank transfer and cryptocurrency are the clear frontrunners in terms of losses. Together, these account for $1.5 billion in stolen funds, more than double the losses from all other payment methods combined. While this is a great deal of money, research indicates that fewer than three percent of consumers report to law enforcement, so the true losses are many magnitudes greater.

Among older adults, as you said, gift cards are still the most common method of money transfer. Gift cards are favored by perpetrators because they are easily available to consumers, they are anonymous, they are instantly redeemable, and have very few controls.

Retail sales clerks are often the only individuals in position to intervene. In my research supported by AARP, my graduate students and I interviewed retail store managers from around the U.S. We surveyed cashiers, and we visited local stores to document what is being done. We found that most major retailers have some type of signage warning customers about gift card scams, but the messages were typically small, they were placed out of eye level or completely lost in the sea of gift cards competing for shoppers' attention.

Less than half the our cashiers we surveyed reported that there were any limits on purchase amounts, and the store managers said that they have not received any formal training from their employers on what to say to intervene. Ultimately, they felt that they are not authorized to deny gift card purchases if the customer insists, even if they are certain it is a scam. As the saying goes in retail: "Customer is king."

In light of these findings, I believe that more education for front-line retail staff is warranted, but more importantly, we need to demand action from the gift card payments industry, including the payment processors and the card issuers. These are the entities that can see when the money is being loaded onto a card by customers in stores and then immediately redeemed by perpetrators in a remote location. Additional controls might include temporary holds on suspicious attempts to redeem high-value cards, and that would give customers more time to identify and report fraud. Lower transaction limits could also reduce the loss amount and just make gift cards less attractive to fraud criminals.

Consumer education is also critical. As we say, forewarned is forearmed. However, we cannot ask individuals to shoulder the burden of consumer protection alone.

In conjunction with education, we need the private sector to step up. Legislation, such as the TRACED Act, is a fantastic example of how phone companies, with help from Congress, can limit unwanted and fraudulent robocalls. We need similar solutions applied to other methods of contact, from bogus text messages to fake social media profiles.

We also need to expand the Senior Safe Act to encourage all types of financial institutions to act quickly by placing temporary holds on suspicious transactions and reporting elder fraud to the authorities.

Last, based on what we are seeing in the most recent reporting data, cryptocurrency is playing an outsized role in the fraud landscape. The fraudsters' playbook has evolved, and they are moving into new, complex, and underregulated environments. Steps need to be taken now to curtail the rise of crypto-facilitated fraud.

In summary, you are so fortunate to sit in this rare area of policymaking where consumers, both sides of the aisle, and the private sector all want the same thing: to stop criminals from exploiting Americans. Let us advocate for greater investment from the private sector and for companies to be proactive when they suspect fraud instead of reactive when the money is already gone.

Through these and other actions, we can show older consumers that the Federal Government is committed to keeping their money safe, holding the perpetrators accountable, and restoring trust in the marketplace.

Thank you.

The CHAIRMAN. Thank you very much, Dr. DeLiema, for your testimony.

We will move next to our second witness, Mrs. Klingler.

STATEMENT OF NANCY PHAM-KLINGLER, SENIOR ADULT PROTECTIVE SERVICE SPECIALIST, COUNTY OF SAN DIEGO HEALTH AND HUMAN SERVICES AGENCY, SAN DIEGO, CALIFORNIA

Ms. PHAM-KLINGLER. Good morning, Chairman Casey, Ranking Member Scott, and members of the Committee.

My name is Nancy Pham-Klingler, and I am the senior adult protective service investigator assigned to the financial unit in San Diego County, California. Thank you for allowing me to join you today to discuss a topic I am passionate about and dedicated to: the fight against fraud and scams.

Over the past year, I have been privileged to be the primary APS investigator attached to the San Diego County Elder Justice Task Force—a partnership of the San Diego County District Attorney's Office, the FBI, local law enforcement in San Diego County, and Adult Protective Services seeking to impact scams against older adults.

San Diego County is home to over 3.3 million people. Of that, approximately 680,000 are individuals over the age of 60. From 2000 to 2030, it is projected that adults 60 and older will increase by 130 percent while the general population will increase just 38 percent. That means one in four San Diegans will be over 60 years of age.

These numbers are real. Adult Protective Services has witnessed firsthand the increase in APS referrals over the years, particularly cases with a nexus to scams and financial abuse. From June 2021 to July 2022, over 1,200 APS scam-related cases were referred to our office with an estimated loss of over $34 million. It is clear we have an issue—an issue that our most vulnerable population, who have spent years and years of hard work saving for their golden years, only to be deceived and have their life savings stolen under false pretenses by vicious perpetrators.

APS frequently is the first to respond to these victims. We help them start the processes to potentially recover their losses, bring some sense of security back, and protect them from future exploitation. During our investigation, we must build a rapport, gain their trust, and assess for safety all while ensuring that we gather all the necessary evidence to bring our cases to the next level.

What is the next level, you may ask. As we know, without evidence there is no crime. Our APS team members, along with our local law enforcement agencies in San Diego have been trained to gather key details such as: How did the scammers contact you? What company did they represent? What account numbers and financial institution were mentioned during your conversation?

These cases are complex. Some of the top scams we see use mobile cash apps, peer-to-peer money transfer, social media engineering, and cryptocurrency. Can we confiscate a Bitcoin machine that an elderly person just walked up to and deposited $25,000 in cash with a QR code that they just received via text message?

As difficult as these cases are, recovery of these funds is potentially possible. One example is as follows:

On July 13, 2021, Adult Protective Services was contacted by the San Diego Sheriff's Department with concerns about a possible local Publishing Clearing House scam victim. There was a $75,000 cash package that was located in Florida that came from a San Diego address. Upon investigating this residence, we located a mailer with our elder's name on it. With the support and assistance of our Elder Justice Task Force, we reached out to the appropriate parties to gather the necessary information to create an APS referral. This referral allowed us to have open communication with the identified victim, speak to their financial institution, locate natural support, and collaborate with local law enforcement. Through this collaborative work, we conducted a records request.

One of the payments was to the San Diego address where the package was sent from in Florida. This victim identified—stated that she had sent over $250,000 to various individuals through the

direction of employees from the Publisher Clearing House scam. This is not an uncommon method of payment where scammers are using our most vulnerable citizens to launder money for them and ultimately requesting for cash payment to be mailed out to random addresses. We worked with the financial institution and reviewed over 271 pages of bank records to confirm that our victim, in fact, sent the money to another senior and that check was cashed by the receiving senior's bank. Collaborative work works.

I am here today to speak to you because this is a national problem crossing State and international borders. In the past year, according to IC3.gov, more than 92,000 victims over the age of 60 reported losses of $1.7 billion, and that is just reported losses. This represents an increase of 74 percent since 2020. This is a crisis, and without swift action the trend will continue.

Reporting on elder financial abuse is mandated. We have infrastructure in place to report scams—IC3, FTC, FBI, APS, and local law enforcement—but what we need is continuous support and additional resources so agencies involved can help solve the greater issue. We need legislation and targeted education that makes it harder for these scammers to attack our precious population in our society and put faith back in our public system, as well as a means to obtain bank records quickly for suspicious transactions.

On behalf of San Diego County, I thank you for bringing this critical issue to the forefront and for your continued work to protect the vulnerable seniors in our community. I welcome any questions the Committee may have. Thank you.

The CHAIRMAN. Thank you very much, Ms. Pham-Klingler.

We will turn next to Ms. Costigan.

STATEMENT OF AURELIA COSTIGAN,
SCAM SURVIVOR, PITTSBURGH, PENNSYLVANIA

Ms. COSTIGAN. Hello. My name is Aurelia Costigan. I was born in Pittsburgh, Pennsylvania. I have been married twice; both of my husbands have passed. I have been widowed since 2008 when my second husband passed. I used to be a school bus driver, and then I also worked in health care for several years. I am now retired on Social Security Disability and Surviving Widow's Benefits. I live in the North Hills with my youngest daughter. I have two daughters, three grandchildren, and two great-grandchildren.

Last September, I got a phone call from the number that is listed on the back of my debit card. This man said he was from Dollar Bank and told me that there were two suspicious activity charges on my account from Tennessee. He said one was from a grocery store and another one from a movie theater. He asked if I was in Tennessee recently and had I made any charges there, and I said, "No, I live in Pittsburgh. I have never been to Tennessee."

He asked if I had any relatives or friends that were there that could have used my card, and I said no, so he proceeded to say that to prevent having to cancel my card and issue a new one, he could help me out with that by adding a Zelle account to protect my bank account. At that time, of course, I had no idea what Zelle was, so I just assumed that what he was saying would be helpful, so I said, "Okay, that is good."

Then he said that had to have some type of proof that he was actually speaking with Aurelia Costigan and he needed some form of identification to prove that he was actually speaking with me, and he asked if I had online banking, but I do not use that. I go to the bank myself personally when I do any kind of banking, so he said, well, the only other option to use to prove who I was - was my Social Security, so not thinking anything, you know, unusual, I thought that sounded feasible. I assumed he was from my bank, and I gave my Social Security number, and I thanked him, and we hung up.

Well, less than five to ten minutes later, my phone starts blowing up. It was notifying me of charge after charge after charge, one after the other. Twenty-two, to be exact. I panicked. I went to my bank, and I told them about the phone call, and they said, "We have no charges from Tennessee on your account." That is when I realized I was scammed.

They said that they would look into it. The manager of my bank said, "I will not quit until I find that money." I was told to notify the police and file a complaint. I did, and also the State attorney's office, which I did. The police officer was very helpful and understanding. He provided me with resources and pamphlets, and he even held my hand and said that he felt for me and other people that are taken advantage of like this.

I was an absolute a wreck. I could not sleep. I had trouble eating. I was devastated. The money I lost because of this scam was $1,800, and that is a lot of money, and it takes me a long time to earn money like that for being on Social Security to be able to save any kind of money. Sometimes you need for car breakdowns or medical expenses that come up.

When these kinds of things happen, you need to have some kind of back-up, and I thought I would never get that money back, but, thankfully, maybe a month or so later, my bank was able to get my money back—all the $1,800. The State attorney's office told me that I was very fortunate that my bank worked so hard with Zelle to get my money back. I felt like I could finally calm down now after a lot of praying.

I know that not everyone has had this experience. These scammers get away with this every single day, and elderly people like myself, we are always trusting people. Don't give absolutely any information to anybody about yourself on the telephone. I now tell my friends and my family my story as a warning. I tell them to be careful, and I hope that we can do something so that this does not happen to anybody else.

The CHAIRMAN. Ms. Costigan, thanks very much for sharing your story. We are grateful for it.

We will wrap up with our fourth and final witness,

Mrs. Fehler.

STATEMENT OF POLLY FEHLER, COMPUTER SCAM SURVIVOR, RETIRED AIR FORCE OFFICER, SENECA, SOUTH CAROLINA

Ms. FEHLER. Thank you, Ranking Member Tim Scott and Chairman Casey.

My name is Polly Fehler. I am 76 years old. I am the mother of two sons, the grandmother of five grandchildren, a retired reg-

istered nurse and a retired nursing educator. I also ran a nursing department that taught RNs for 5–1/2 years, so I have a lot of compassion for people that have to do budgets and handle money, and I felt that I was very fraught with some knowledge there.

My husband of 48 years died nine years ago. I have lived in the same house, as Senator Scott said, for 32 years, and I am here today to tell you about the scam which upended my world last year.

I have always paid my bills on time and managed to pay our house off early. I have worked hard to maintain a thrifty lifestyle. I taught our sons the same. I pride myself on not spending foolishly and on having sharp financial instincts, but when I realized what had happened to me, that somebody actually took such advantage of me, the bottom fell out of my life.

I had been having email trouble with my old computer, but it was in the middle of the pandemic, so I could not get it fixed. No one would come to the house. I could not take it to the local Staples. In January 2021, things started to loosen up a little bit, and I went and bought a new computer. Things were going back to normal.

On April 13th, I was using my new laptop on public WiFi, and suddenly a pop-up appeared on the home screen. It was a large orange blinking triangle, and, of course, it is going to take your attention, and it said I have computer problems; my computer had been compromised.

I called the listed number because I was afraid I was in for the same kind of problem I had had before, which had cut me off from my community and my church. A reassuring voice alleging to be a representative of Microsoft answered. He told me if I bought their protective software at $299, which included computer monitoring for two years, that he would gee that he would call me every so often, and he did. As far as I could tell, this was going to be good customer service.

The third call later, in June, on June 14th, this man who was calling said he wanted to check on the program and see how it was working. If it was not working, he wanted to refund my $299, plus give me $100 for the inconvenience of bothering him, so to run the software, he wanted me to go to my computer and turn it on. I did. I had to give him full access. During this test message, other messages flooded the screen and kept rolling by, and there it was again: an alert claiming my computer was compromised. I told him to send the refund by way of check to my home address, and he said he could not. The service had been paid for electronically. They were going to return my money electronically.

He moved to a different browser window, and the screen broke out into chaotic movement with numbers coming, rolling around and around and around. Then all of a sudden everything stopped, and the number on the screen with other numbers, but the number highlighted was $20,000. The scammer feigned outrage, saying I intentionally stopped the computer when my checking account reflected a $20,000 deposit. I did not know what he had been doing on there, but I could not see any alleged moneys he was talking about. We were not in my bank account; we were not in my check-

ing account. I never had touched the computer or the mouse while he was running his testing.

Then he showed me, he opened the window and showed me my checking account. Instead of $6,000, it had $26,000 in it. I screamed: "How did this happen? How did you get in?" I was stunned. I had a balance that was way above what I should have had, and it was not mine. Being so precise about moneys, I had no idea where the money came from. I wanted nothing to do with it. The scammer was furious, demanding that I pay them back immediately. Microsoft would sue me, would send me to collections, would get the police after me, would ruin my credit, and I had worked hard to try and establish a good credit rating. I was terrified. I felt the only way I could get my money back was to do exactly what he said.

He told me to wire the $20,000 to a Microsoft subsidiary in Vietnam. The instructions were to tell USAA, my bank, that I knew this person and owed them $20,000. He told me not to veer off those instructions or I would not be able to pay them back.

After I completed the wire transfer, our call ended. Immediately I contacted USAA to report what had happened. A representative told me she thought I had been scammed, but I would not get a call back until the next day. This happened now. Why couldn't they call me now? It was after office hours.

The next day, a fraud investigator called and asked what I had done on my banking—in my bank the next day, and I told him, and I did not know anything about what actually happened. They could see that I had taken out $20,000 on my home equity line of credit. I had not opened that line of credit for 17 years. It had been inactive, dormant. I never knew the money was from USAA. I thought it was from Microsoft. I did not know it was a loan for me and that I was throwing it away.

Now, I owed USAA $20,000 plus interest. I live too on a fixed income. I could not make the payments. I could not—the interest even was starting to pile up. At first they told me not to pay any attention to it because it was a fraud investigation, so I did not start to pay it when it was $3 and something the first few days. I did not pay it back, and then it got bigger and bigger, and I could not handle everything.

Finally, after the overdue notices I was getting for the loan, a scary letter came from USAA telling me that I was eligible for bankruptcy. I owned my house. I owned my car. I should not be eligible for bankruptcy.

In the end, this year, not having—USAA put a lien on my house, and not having the moneys to pay it, I had to sell off my Individual Retirement Account in order to pay USAA because it was driving me mentally insane. The situation snowballed. I could not find legal advice. I called the FTA. They took a statement. They never called me back. They were going to. I called the police. I called numerous law firms. I called the South Carolina Attorney's Office. I called many, many places. I did not know about the number that you said now has been in effect ten years and I could call for help here. I have it written down.

I did not find anyone—I was afraid to tell everyone. I did not find anyone to help me until a local reporter, TV reporter, Diane Lee,

came on board and listened to my story and broadcast it. I was afraid of it. I did not want other people to know. I had not even told my son for days, and my second son in Texas for months, because I was afraid of their reaction because I was so stupid. I was blaming myself.

After suffering through the scam, I not only was alone and depressed; I even lost my spirit to live. I sat alone, I hated myself. Some days I could not get out of bed. I thought this is so ridiculous. I went to the VA for medication. I am a vet. I went to the VA for medication. I opted out of all my community and church activities, which before had been a vital part of my life. I had no leadership roles. I did not even attend church after awhile. I could not function as the person I had been. I was not the person I had been.

I am here today because I am a survivor. God is giving me the strength to reclaim my life, and I want others to know there is hope out there. I want others to know that this unmatched misery does not have to happen. Saving others from falling into the pit that I was in that comes with losing your self-worth and retirement savings in a click needs to be done, and we need to do everything we can. I have some ideas, but we will talk about those later.

Thank you for listening, and I look forward to your questions.

The CHAIRMAN. Well, Mrs. Fehler, thank you so much. I think we are all indebted to you for your testimony and your willingness to share with us. I know it cannot be easy to relive some of that horror, and we are grateful you are willing to do it to help others.

We are going to go to questioning in a different order. I am going to turn first to my colleague Senator Blumenthal, and then we will pick up from there.

Senator BLUMENTHAL. Thanks very much, Mr. Chairman, and thank you for having this hearing.

As the witnesses have observed, and I think the Chairman as well, fraud affects elders more frequently and more devastatingly than anyone else, and, Ms. Fehler and Ms. Costigan, thank you for telling your stories with such bravery and precision, because I think they give a voice and face to this problem. It is truly moving, and you have shown not only the financial impact but also the emotional and psychological impact.

In Connecticut, the Department of Aging and Disability Services is warning seniors against genetic testing fraud aimed at Medicare beneficiaries where scammers pose as genetic testing company representatives. They offer free genetic tests and then steal their medical identity in order to falsely bill Medicare, thereby draining the system of needed funds. The supposed free genetic tests obviously are a ruse. This example is only one of many that consumers have reported to us affecting elders, and it is why I was proud to introduce the Elder Abuse Protect Act of 2021. This legislation builds on the Elder Abuse Prevention and Prosecution Act, a bill that I sponsored and helped to pass into law. It provides statutory authority for the Elder Justice Initiative, which coordinated activities at the Department of Justice to combat elder abuse, neglect, and financial fraud.

The Chairman is to be commended for his leadership in this area, as is the Ranking Member, and it brings us here today.

Dr. DeLiema, I was especially interested, as a former Attorney General and also a Federal prosecutor, in your data and statistics on which frauds affect seniors most commonly, and, of course, they evolve, as you observed, for example, the use of Government agencies as a means to entice or deceive seniors, different Government agencies over different times, but I was particularly interested in your information about romance schemes and scams. I want to demonstrate my perhaps naivete and ignorance by saying I really had no idea that the magnitude of loss was greatest for those 70 to 79 and 80 and older, and I wonder if you could expand a little bit on what you have told us in your testimony about the reasons why that amount is at $10,000; whereas, for young people my children's age, between, let us say, 20 and 29 or 30 and 39, the amounts are much less. I do not know whether the frequency is higher, but the amounts are less. If you could explain?

Dr. DELIEMA. Absolutely. Thank you, Senator, so romance scams are unique in that they tend to go on for many weeks, sometimes many months, so when a person finally does report, the magnitude of total losses is reflected in the report, so, typically, perpetrators do not just start right off the bat asking for $10,000 from their romance scam victims. They might ask for smaller amounts, and then once that trust is built, then they will start asking for greater and greater sums of money, so that is why I think we see those amounts so high.

It is possible that younger adults might have more people in their lives to intervene and say, "Hey, this seems suspicious"; whereas, for older adults with greater isolation, it can go on for longer, but the fact that they are not losing, you know, the $10,000 all in one fell swoop indicates to me that there are so many opportunities for intervention along the way, like let us see if we can catch those smaller amounts of money leaving first to really prevent the deep pockets from being lost.

Thank you.

Senator BLUMENTHAL. Presumably also minimize the emotional impact if it is caught earlier.

Dr. DELIEMA. Absolutely. You know, perpetrators' MO is to tell the person to keep these relationships private. They will say things like, "Your children will not understand." You know, "This is between us." Again, you know, one of our questions is why don't they reach out to their friends or family members, and it is because they are instructed not to.

Senator BLUMENTHAL. Thank you. Thank you very much. Thank you all for your testimony. This is very, very helpful and valuable to us. Thank you.

Thanks, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Blumenthal.

We are also joined by Senator Gillibrand and Senator Braun. We will now next turn to Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman. I am so glad that you and the Ranking Member are continuing the Committee's focus on scams that are directed against our older Americans. It is extraordinary how painful, not just financially but emotionally, these scams are.

In that regard, I want to thank Mrs. Costigan and Mrs. Fehler for coming forward and sharing their very powerful stories that will help to educate other older Americans and tell them that they are not alone and that they should get help and, most of all, help them avoid these scams in the first place.

Mrs. Fehler, I want to start with you, and, again, I found your testimony to be so compelling because, as you pointed out, you have an extensive financial background, and you are not easily deceived, but you fell prey to an extremely sophisticated, ruthless scam that went on for months, and for those of us—and I put myself in that category—who are not that savvy technically, getting a notice on your computer that it has been compromised would cause alarm for almost all of us.

Over the past several years, the Aging Committee has held many hearings examining scams that are targeting older Americans, and what we have frequently heard is that if anyone had intervened at any point in the process, the scam would not have been successful. The Senior Safe Act that I introduced with Senators Casey and Scott, was signed into law in 2018. I know one of our witnesses has urged an expansion of that, which I think is worthwhile, but the whole idea was to train financial institutions' employees to be able to spot and report financial exploitation of older Americans.

My question for you is, If someone from your bank had seen this very suspicious transaction, where you are opening up a line of credit that you have not used in, I think you said, 17 years and asked you about it, would that have stopped the scam?

Ms. FEHLER. Yes, and they would have stopped it on any level. They could have emailed me. They could have texted me. They could have phoned me. If I go on a trip and I use a credit card and I have not let USAA know that I was traveling to a different State and I used it at a gas station, the first gas charge might go through. The second time my card would have been frozen. That is $20. We are talking about $20,000, and they did not find that I had a right to expect notification. I did not expect a notification because I had not used it. I thought it was closed. I had no use for it, but that is one thing they can do.

I think it is very important that not only seeing the money being moved but seeing accounts being utilized that were not opened before is very important in the education that we give the bankers also, or any financial institution. I think that we need to understand the difference between a scam and fraud. They did not pay mine because they said it was a scam. I have the definition here that the banks use for scams versus fraud, and I believe it was a fraud, but the reason they gave it to me, they would not accept it, is that they said this is a scam, this was totally up to you. I sent the money. I agree with that. That was stupid, but I did that, but I did not contact me. I did not move my money. They allowed that guy to get into my bank account and move the money from USAA's loan department into that home equity loan, and I had no knowledge of it.

Senator COLLINS. It seems to me that your analogy with the use of a credit card is a very good one. If you go out of the country and you have not told your credit card company, they are likely to decline the transaction and text you or contact you in some way to

find out is it really you using that card, and it seems to me that this was so out of your normal practice that your bank should have realized that it was suspicious and contacted you, and that is what Senior Safe is all about, is to ensure that banks are not violating privacy laws or they also are not going to be held liable in some way for asking you is this really a transaction that you want, so thank you for sharing that experience.

Thank you, Mr. Chairman.

Ms. FEHLER. Can I say one other thing? I was a member of USAA for 41 years, and I felt, I still feel that they owed me something of communication.

Senator COLLINS. I agree.

Ms. FEHLER. Thank you.

The CHAIRMAN. Thank you, Senator Collins.

I will turn next to my questions. I want to direct my first question to both Ms. Costigan and Mrs. Fehler. As I indicated earlier, and several of us have, you have shared very personal stories, and we are grateful for that. I wanted to note that part of what your testimony indicated about the impact on each of you individually, Ms. Costigan talked about being devastated, but then, thankfully, when the money was returned, she could calm down, but, Mrs. Fehler, so many times in your testimony you talked about the impact on you, that you said, "The bottom did not just fall out of my life. I had dropped straight into Hell." You talked about being depressed and alone and that you could not function and so many other expressions of the horror you were living through.

I guess because of that, it cuts through for a lot of Americans who will hear your testimony, and it allows people to understand that this can happen, as Senator Collins said, to any of us, no matter what our background is or no matter what our age is.

For both of you, your testimony highlighted the importance of not just helping people to spot so-called red flags, but how to respond, to make sure there is an adequate response when you do point to that red flag. This year's Fraud Book focuses on both, and I think that is one of the real benefits of it.

I guess we will go in alphabetical order, Ms. Costigan and then Mrs. Fehler. Why is it important to focus not only on education to prevent scams, which is obviously very important, but also on resources to respond and to help when the scam actually occurs?

Ms. COSTIGAN. Well, I feel it would be a little bit of both, actually, what you are saying, because people of our age, at our Baby Boomer age, we were very trusting persons. We are also not tech savvy on computers, in the computer world, which makes it a lot harder for the elderly people, so that needs to be brought to attention as well to train elderly people on how to handle that with computer work.

I feel for Mrs. Fehler because the $1,800 I lost, which thankfully my bank was able to recover, to me $1,800 was like having $18,000 taken from me, but for Mrs. Fehler, my heart goes out to you for what happened to you, and this needs to be made very more publicly as to this happened in this world, which is very sad that people are taking advantage the way they are.

Ms. FEHLER. Thank you.

Chairman CASEY. Mrs. Fehler?

Ms. FEHLER. I believe that we need more resources in the ability to not have the victim feel that they are totally at fault. The first thing you do is you may lash out in anger at the people that are doing it, but then that is cutoff. You do not have any more to do with it. Then they have put the blame on you, and you carry that blame, and you are afraid to tell people, you are afraid to tell your family, because if you are to blame, how can you take any more pressure? How can you do any more than what you are doing?

The Seneca Police Department came over and talked to me and told me they could not do anything. They told me that it would not do any good to go to the county sheriff's department, it would not do any good to go to the State department of law, that I needed to get a hold of some legal people, and I went through very, very, very—a lot of people, and it was all I could do. I might be able to make two phone calls a day, and then I was totally mind-set wiped out, and I think that we need to be able to allow the plight of senior citizens to also reach the families and the friends around us, because we are so afraid of not being able to fill our need as a person that has had experience. We are so afraid of being labeled. We need someone that can help and push us on our way and know what some of those resources can be, because, frankly, I am just astounded that all the people I talked to, not one of them gave me the number for the resource line. Not one. Not the Federal Trade Commission, who I talked to for a long time, they never—they said they would call me back. They never did. Not the South Carolina legal assistance. I talked to them once. They never called—they never got me back in. Nobody got us back in to help.

It is important that we educate the seniors. One faulty thing about seniors, one problem with seniors is that some of us are not so alert and active and able to understand. We need somebody that knows where we are at mentally and physically that can tell us the kinds of things that we can do where we are. If our mental acuity is not quite as good, we need somebody that does not make us feel that we are no good, and they need to know the resources, so it is really important, this book is really important, the number is really important to get this information out, but I get turned off when nobody calls back and they say, "We will get right back with you." Or get their name and number, you try and call back, and they are not available, they are not available, they are not available. I think that that is horrible. There needs to be a person that is going to answer, and you need to know who they are, and they need to hold some accountability for those resources if they are going to do something.

The CHAIRMAN. No question that it is not good enough for us at a hearing like this to point out the problem. We have got to be determined to get every level of government to up their game, every local agency of government, county, State, Federal. Everyone has got to do more to respond so you do not have that experience of being victimized and then kind of further injured by a lack of response.

I have a question, which I will wait for the second round, to Ms. Pham-Klingler. I will turn next to Ranking Member Scott.

Senator SCOTT. Thank you, Mr. Chairman.

I am going to ask a question of Ms. Aurelia Costigan. Older Americans are a popular target for scammers. One reason I am a cosponsor of the Empowering States to Protect Seniors from Bad Actors Act, this bill provides $10 million in grant money to State regulators to help protect seniors from fraud.

Looking back on your experience, what are some of the red flags and your tips you would like to share with other seniors that may help them identify possible scammers?

Ms. COSTIGAN. When people call you on the phone and they ask you questions, do not answer them. If you have any confusion about it, go to your bank and talk to them in person. Do not give any information out on the telephone such as Social Security numbers, online banking numbers, anything of any kind, because I have learned my lesson.

Senator SCOTT. It is incredible that we find ourselves in a place where you have to really question everyone that calls our seniors. It is just an unnerving position for seniors to find themselves in, that literally sincere people who are looking to be helpful and just to do the right thing have to rewire the way they see the world because of the scammers and fraudsters. It is a different kind of evil for those folks who take advantage of our seniors in vulnerable positions.

Mrs. Fehler, I was walking back from my Banking hearing where I was asking questions and ran into Mrs. Collins, who said that you were simply spectacular. She really found your testimony and your responses to her questions to be illuminating and helpful, and the complexity of the scam as she heard you articulate it was one that was just unbelievable from her perspective, so she was really impressed.

You may have answered this in part based on my talk with her, but I do think that seniors benefit from hearing your tips, a similar question that I asked just now. I would love to hear your answers to how do we help seniors in such a situation. Yours was so complex. How do we find those red flags and warnings? What tips would you provide?

Ms. FEHLER. Well, one thing that is really important, and I kind of alluded to it at the end of my last statement, but I think that—let me give an example. USAA is a Federal bank that I belonged to, like I said, for 41 years. I never talked to the same person over the more than 50 calls I made except for one time. His name was Jim. I always had to go through what had happened. They had notes. They either had to read them or they had no questions or they could not get me to the person.

When USAA sent me a letter, it was signed by a man that I could file for bankruptcy. I tried to get a hold of that man. They would not put me through to him or his office. I said, "Does he exist?" They said, "Well, we think so." I never was able—because USAA comes out of Texas.

Senator SCOTT. Yes, ma'am.

Ms. FEHLER. I never was able to talk to anybody, to know anybody, so I was really—when I got back and was able to function, I was really able and happy to be able to go to a small bank—it is Wells Fargo, it is a huge bank, but a small banking bank, and they took me right in. They talked to me. They introduced me to

the people that would be handling my account, and when I had the problem where I was so depressed and I did not know what to do with this loan I could not pay off, they got me into the people that handle your funds, my retirement funds, and the two of them together talked to me and determined that my mental health would be much better if I could get this loan paid off, and what would be the best way for me to do that without causing the most loss, because I lost more money than $20,000 by canceling an IRA, and to have that kind of care from a financial institution was what I had been looking for.

USAA, before, I touted it as a great, great place, but you need someone that knows you and listens to you, and they need to get their act together, and there are millions of USAA members that are not going to be met—their needs are not going to be met if they do not get their act together, and they did not listen to me at all.

Senator SCOTT. Thank you very much, and with the little time I have left, I want to followup with a question to Dr. DeLiema, because it really is my next question, which is the mental health consequences and your research on that. Can you just spend maybe 30, 40 seconds giving me a synopsis?

Dr. DELIEMA. Right. I have had the privilege to read consumer complaints on fraud through my Special Government agency position with the Federal Trade Commission and also in interviews with victims, and I have had to take breaks when reading or listening to their stories about what happened. I have had to just step aside, do something else, go for a walk around campus, because it is painful. You know, people talk about their marriages collapsing when the partner found out, and they talk about depression, and they talk about trying to take their own lives.

We should not just think about financial crimes as being, oh, these have small impacts. The impacts are as severe as victimization by physical and sexual assault.

Senator SCOTT. Thank you very much. That is powerful. My goodness.

The CHAIRMAN. Thank you, Ranking Member Scott.

I will turn next to Ms. Pham-Klingler for a question. For community education, which I know you know something about, for that to be effective, it has got to reach all communities, of course, and that is why Ranking Member Scott and I made it a priority to ensure the Committee's fraud resources are available in both English and Spanish. While that is an important step, we know that there is more work we have got to do together. There are so many seniors, particularly those in diverse communities, who are not receiving the information that they need.

The Federal Trade Commission's Scams Against Older Adults Advisory Group that I mentioned earlier has an important role to play in identifying solutions to reach every senior, every senior who needs tools, information, and support, so I would ask you, do you have any advice for the Federal Trade Commission and the Council itself as it begins its work to ensure that their work takes into consideration the following: language, accessibility, and other needs?

Ms. PHAM-KLINGLER. Senator, thank you for your question. My advice would be the methods that we are using to reach our targeted audience, the same methods that these scammers are using

to perpetrate our victims, such as online, where they frequent most, social media platforms, reaching out to family friends, and allowing this to be a more normalized conversation among each other, and also to provide this in multiple languages in communities that are less willing to speak up about being a victim of a scam.

Thank you.

The CHAIRMAN. I know we are going to turn next to Senator Rosen. Senator Rosen I think it might be available virtually.

Senator ROSEN. I am here. Thank you, Senator Casey. I appreciate it. Of course, I am not in the room, but I think Senator Scott is there. I really appreciate you both for holding this really important hearing. These stories are heartbreaking, devastating, and we really need to do something to protect people, because they do not happen just in one community or another. They are happening in, of course, my home State of Nevada, but all across the country, and bad actors that continue to target and scam Nevadans, particularly our Nevada seniors, and, in fact, according to data from the Federal Trade Commission, scams cost Nevadans nearly $36 million in 2020 alone. ID theft fraud remains the top type of scam targeting Nevadans, much of it done through phishing and phone calls, and particularly worrisome to me is that scammers are increasingly holding onto personal data for long periods of time, even up to a year or two after obtaining it, leaving seniors and others kind of in the dark as to when their data might be used. In some cases, we are witnessing scammers utilizing data obtained in the early days of the pandemic.

Ms. Pham-Klingler, I am told by AARP Nevada that delayed use of data obtained via scams is really becoming a problem in our State, and so what should Nevada seniors who may have been a victim of a scam in the past and they say a lot of time has passed by, I may not have to worry, how do they protect themselves now considering that people are using their data now or might use it in the future?

Ms. PHAM-KLINGLER. Thank you, Senator, for your question. My advice and my encouragement is for them to safeguard all their banking information, changing bank account numbers, monitoring their credit, and ensuring that there is an alternative person who has oversight over their finances, such as a loved one or someone that they trust has a secondary eye on their banking stuff.

Thank you, Senator.

Senator ROSEN. Thank you. I want to move to something else that really happens a lot in Nevada—I know it happens across the country as well—particularly after disasters, are these home repair scams, because according to the Nevada State Contractors Board, since the beginning of the pandemic, there has been a marked increase in complaints to the board about unsolicited individuals, you know, they just go door to door in my town and all across Nevada. They claim to be contractors. They offer home repairs at lower rates, but, actually, they are unlicensed, and they put high pressure tactics for people to put money up front. They leave no paper trail. They gravitate to some of our communities where the English language is limited English proficiency, and that compromises a lot of groups in Nevada.

Dr. DeLiema, are you observing home repair scams across the country as well, particularly in the wake of natural disasters, other events exacerbated by climate change, with a lot of wildfires, of course, up and down Nevada and across the West? How is the FTC responding to these, and particularly for those with limited English proficiency?

Dr. DELIEMA. Thank you for your question, so scammers flock to areas where there is disruption. Where there is confusion and fear, that is just a playground for fraud criminals, so while I cannot speak from the perspective of the FTC, I can say that when we think about consumer education, education is best delivered in the moment that it is most relevant, so when there is a natural disaster, that is the time we need to alert those communities to the fact that there will be criminals. There will be people going door to door to try to take advantage of them at a time when they are hit hardest emotionally, so, you know, we need to inform people to not do business with someone who comes to you. Do your due diligence, so thank you for that question.

Senator ROSEN. Thank you.

Thank you, Chairman Casey. I yield back.

The CHAIRMAN. Thank you, Senator Rosen.

We are coming to the end of our hearing, and I wanted to start by thanking our witnesses. I will have a closing statement; then I will turn to Ranking Member Scott.

We cannot thank our witnesses enough for their testimony today, bringing either personal experience in the case of Ms. Costigan and Mrs. Fehler, but others bringing experience as advocates, as experts. The combination is very helpful for not only the Committee, the members of the Committee and our staffs, but for the American people.

We hope that a hearing like this and the work that was done to put together our "Fighting Fraud: The Top Scams in 2022," that this work will lead to people being more and more aware and to prevent these scams from occurring, and also to get the help they need when and if a scam does impact their lives.

Your stories and those of others who have appeared before this Committee further demonstrate our determination to prevent these terrible scams in the first place and to bring justice, swift, significant justice to the criminals who engage in this conduct. No one should lose a single penny of their hard-earned money to a con artist, and that is why I was proud that Congress passed the bipartisan Stop Senior Scams Act to ensure we can develop the tools and resources to prevent seniors from becoming victims of these crimes. It is also why Ranking Member Scott and I have worked closely to release the revamped Fraud Book that I just made reference to both in English and in Spanish to ensure seniors have the tools and information that they need.

I look forward to continuing this bipartisan work together, and I now turn to Ranking Member Scott for his closing statement.

Senator SCOTT. Thank you, Mr. Chairman, for holding such an important hearing on a topic that really is heart-wrenching. Thank you to each of the panelists for taking your time and investing your energy and your expertise on such an important topic.

Mrs. Fehler, thank you so much for spending your time here and representing our State so well.

Ms. FEHLER. Could I add one comment, sir?

The CHAIRMAN. Sure.

Ms. FEHLER. Thank you, Chairman Casey. I think that if an independent organization could hear appeals from people who have been denied reimbursement, when the bank themselves makes the decision that this is not viable, they are the ones losing the money. Of course, they are going to lean toward that. That is a biased finding. Is there any way we can make them have an independent organization that would overview anybody that wants to appeal one of their decisions? If we could look forward to something like that, that would be great.

Thank you.

The CHAIRMAN. Thank you, and we will certainly take that into consideration. We learn a lot from these hearings, and we also get a lot of good ideas, so we are grateful that you are sharing that.

Senator SCOTT. Absolutely.

Ms. FEHLER. Sorry to interrupt.

Senator SCOTT. No, ma'am. If I am going to be interrupted, at least it is by a South Carolinian. Thank you very much. I appreciate that. Necessarily so sometimes.

Most of my good ideas, Bob, come from people in South Carolina, not from my own cranial cavity, so this is good news that continues to show fruit.

855–303–9470. The one thing I will say that is important, I thought having the Chairman mention the number twice during his opening comments and me mentioning the number at least once or twice was good enough, but after listening to the testimonies and after hearing how hard it is to coordinate and to have collaboration on the parts of our seniors who are in desperate straits, I do not know that you could say the number often enough, so I will say it one more time: 855–303–9470.

Mr. Chairman, I will just close with this comment as opposed to going through my prepared remarks. Inflation is sky high. Nest eggs are being hammered. Our seniors cannot afford $1 billion—$1 billion—of lost money because of scams. It is unconscionable. I believe that the testimonies that we have heard today will help seniors keep more of their money and hopefully put up a firewall to the scammers and fraudsters who are taking too much of the resources of people who work their entire lives to have them.

Thank you all for being here with us today.

The CHAIRMAN. Thank you, Ranking Member Scott, and thanks for referring to the number again. I will read it one last time just so that we have said it approximately an equal number of times: 1–855–303–9470, and I want to thank the Ranking Member for emphasizing that.

I did not acknowledge one of our Senators who was with us today as well. Senator Warnock was with us as part of this hearing, and I wanted to note as well, I want to thank both of our staffs for working on this book. This is new and improved, and I said it is in both English and Spanish, but just give people seeing the hearing some sense of what is inside, just to give an example, for exam-

ple, the number one scam in the top ten is Government imposter scams, so the summary of that appears on page 15.

Right after that, you have a section called "Red Flags," which are things to look for, but maybe most important is the steps to prevent and respond, and I think that is very important for people to take a look at.

The first step to prevent and respond is if someone calls and let us say it is a Government imposter scam, hang up the phone. Hang up the phone and do not reply to the email, so it goes on from there giving other advice, but it is very practical and it is important that we have data about how many of these scams occur, but it is even more important that we give information about how that individual should react in the moment, and so we are grateful that our staffs worked so hard on that.

I want to thank again all of our witnesses for your testimony, whether it comes from your personal experience of having been a victim or your own work and scholarship and advocacy. Both are so valuable.

I want the Senators to know on the Committee that if any Senator has additional questions for the witnesses or statements to be added to the record, the hearing record will be kept open for seven days, until next Thursday, September 29th.

Thank you all for participating. This concludes today's hearing.

[Whereupon, at 11:21 a.m., the Committee was adjourned.]

APPENDIX

Prepared Witness Statements

School of Social Work
College of Education and Human Development

UNIVERSITY OF MINNESOTA
Driven to Discover®

WRITTEN TESTIMONY OF DR. MARTI DELIEMA

submitted to the

UNITED STATES SENATE
SPECIAL COMMITTEE ON AGING
on

Stopping Senior Scams: Empowering Communities to Fight Fraud

September 22, 2022

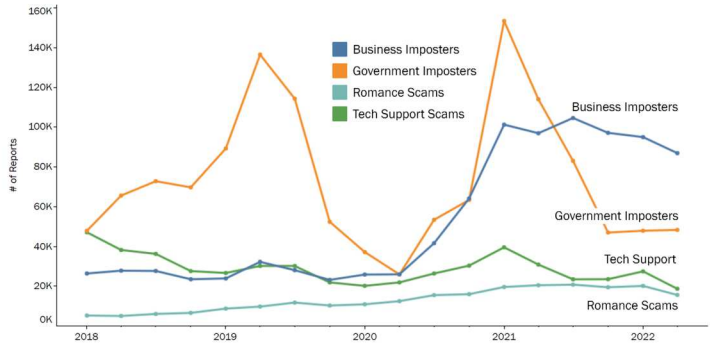
Marti DeLiema, PhD
Assistant Professor
University of Minnesota School of Social Work
mdeliema@umn.edu

Good morning. Thank you, Chairman Casey, Ranking Member Scott, and members of the Committee. My name is Dr. Marti DeLiema and I am an Assistant Professor at the University of Minnesota School of Social Work. I conduct research on consumer fraud and strategies to safeguard older Americans' financial security.

You have invited me today to describe current trends in consumer scams affecting older adults. I will start by stating the fraudster's playbook is in constant evolution. While core persuasion tactics remain the same, perpetrators routinely experiment with new storylines, new entities to impersonate, and new contact methods to outcompete consumer education and law enforcement efforts. Anyone, regardless of age, may be targeted by fraud, and many consumers are bombarded by fraud attempts multiple times a day.

We can use consumer complaint data compiled by the Federal Trade Commission (FTC) to explore current trends. Government imposter scams have been in the top five most reported categories of fraud affecting older adults for multiple years in a row,[1] but the government agency being impersonated has changed over time— the IRS, SSA, FBI, CMS, USPS, and so on. The challenge is to predict which agency's clothes the perpetrators will try on next, and to create consumer education campaigns that are robust to these changes.

Figure 1. Prevalence of imposter scams reported by consumers, 2018 - 2022 Q1, Q2



Data source: Federal Trade Commission Consumer Sentinel. (2022). Available at https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports

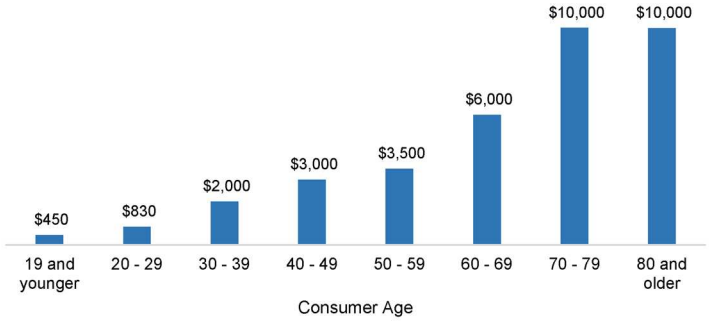
Throughout the pandemic, business impersonation scams grew exponentially, particularly retail company-imposters. Some of these scams start with a text message, a solicitation method that is much harder for consumers to authenticate. As online purchasing took off in response to social distancing, perpetrators took advantage of Americans' fear, confusion, and supply chain

[1] Federal Trade Commission (2022). *Age and fraud loss infographic.* Available at https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic

shortages by using a rash of online shopping scams. Older Americans, some with limited technological proficiency before the pandemic, turned to their personal computers and other digital devices to stay connected. Once again, scammers seized this opportunity to perpetrate new variations of the tech support scam.

Romance scams lead the pack in terms of personal financial costs. In a study I conducted with the FTC, we found that median reported losses for consumers in their 70s and 80s were $10,000, quadruple the losses reported by young adults. Romance scams can go on for many months, and perpetrators not only rob survivors of their retirement security, they completely shatter their social and emotional well-being.

Figure 2. Median reported losses for romance scams by consumer age, Nov 2020-Apr 2022

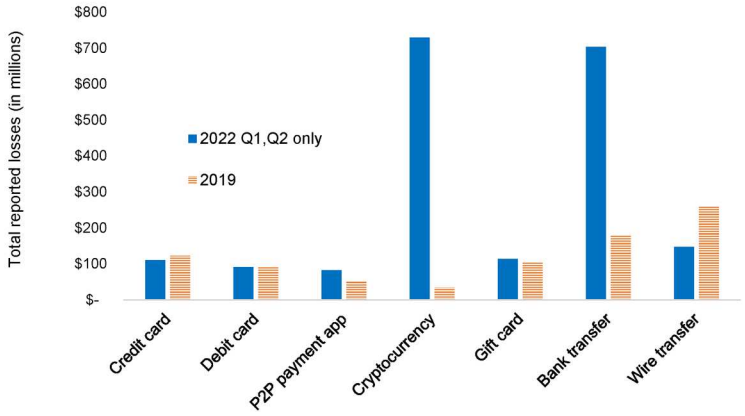


Data source: DeLiema, M., & Witt, P. (2022). Profiling consumer fraud reporters: Demographic characteristics and emotional sentiments associated with victimization. Available upon request from mdeliema@umn.edu.

In 2019, wire transfer was both the most common method of money transfer, and was associated with the highest losses. Today, credit cards are the most common method overall, but bank transfer and cryptocurrency are the clear frontrunners in terms of dollars lost. Together, these money transfer methods account for almost $1.5 billion in reported losses, more than double the losses from all other payment methods combined. While this is a great deal of money, research indicates that fewer than 3% of consumers report to law enforcement,[2] so true costs are many magnitudes higher.

[2] Anderson, K. B. (2021). To Whom Do Victims of Mass-Market Consumer Fraud Complain? Available at SSRN: https://ssrn.com/abstract=3852323 or http://dx.doi.org/10.2139/ssrn.3852323

Figure 3. Total reported losses by payment method in 2019 versus 2022 (Q1, Q2 only)



Data source: Federal Trade Commission Consumer Sentinel. (2022). Available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts

If we shine a spotlight on adults age 60 and older, gift cards are the most common money transfer method. They are used in a wide variety of scams, from government imposter to prize, sweepstakes, and lottery fraud. Gift cards are favored by perpetrators because they are easily available to consumers, anonymous, instantly redeemable, and have very few controls.

AARP recently conducted a survey and discovered that one third of respondents were targeted by a scam demanding gift cards. Of those who were targeted, a quarter complied with the scammers' request. In gift card-facilitated frauds, retail sales clerks are often the only individuals in position to intervene. In my research supported by AARP, my graduate students and I interviewed retail store managers from around the U.S., surveyed cashiers, and visited local stores to document what is being done to educate and protect customers.[3] We found that most major retailers had some type of signage warning customers about gift card scams, but the messages were typically small, placed out of eye level, or were nearly invisible in the sea of cards competing for shoppers' attention. Less than half of surveyed cashiers reported there were any limits on purchase amounts. The store managers we interviewed said they have not received any formal training from their employers on how to detect scams or how to effectively intervene. Ultimately, they said that they are not authorized to deny a gift card purchase if the customer is

[3] DeLiema, M., Sagnes, M., Hanson, W., & Bailey, D. (2021). Protecting Retail Customers from Gift Card Payment Scams: A Three Part Investigation. Report prepared for AARP. Available upon request from mdeliema@umn.edu.

insistent, even if they are certain the customer is involved in a scam. As the saying goes in retail: "customer is king."

In light of these findings, I believe that more education for frontline retail employees is warranted, but more importantly, we need to demand action from the gift card payments industry, including payment processors and card issuers. These entities can determine when money is loaded onto gift cards by customers in stores, and then redeemed immediately by scammers in remote locations. Additional controls might include temporary holds on suspicious attempts to redeem high-value cards remotely. This would give customers more time to identify and report fraud. Lower transaction limits could also reduce loss amount and make gift cards far less attractive to scammers.

Fraud victimization exacts a significant social, economic, and financial toll

Reports of consumer fraud have risen substantially every year, and so have the costs. But true costs extend beyond personal financial losses. In my research analyzing consumer complaints and in interviews with fraud survivors, I learn about survivors' feelings of shame, self-blame, anxiety, estrangement from friends and family members, and even thoughts of suicide. We have yet to quantify the societal and economic impact of fraud including diminished consumer trust in retail companies, in financial institutions, and in law enforcement's ability to bring criminals to justice and provide redress to those who are harmed.

Policy recommendations and future directions

What steps can we take to protect older Americans from fraud? Consumer education is critical. Research has shown that educating individuals about scams in advance of them being targeted significantly reduces the risk of victimization.[4,5] In other words, "forewarned is forearmed." However, we cannot ask individuals to shoulder the burden of consumer protection alone. Scams will continue to take new forms, and we will never be able to warn every consumer about every new variant of fraud.

In conjunction with education, we need the private sector to step up to help safeguard Americans. We are fortunate to sit in a rare area of policymaking where consumers, along with public and private sector entities, all want the same thing—to stop criminals from taking advantage of Americans and eroding consumer trust. Legislation, such as the TRACED Act, is a fantastic example of how phone companies, with help from Congress, can limit unwanted and fraudulent robocalls from ever reaching consumers. We need similar solutions applied to other methods of contact used by perpetrators, from bogus text messages to fake social media profiles. As a second line of defense, we need to expand the Senior Safe Act to encourage financial institutions to act quickly by placing temporary holds on suspicious transactions and reporting elder fraud to the proper authorities.

---

[4] DeLiema, M., Li, Y., & Mottola, G. R. (2021). Correlates of Compliance: Examining Consumer Fraud Risk Factors by Scam Type. Available at SSRN: https://ssrn.com/abstract=3793757

[5] Scheibe, S., Notthoff, N., Menkin, J., Ross, L., Shadel, D., Deevy, M., & Carstensen, L. L. (2014). Forewarning reduces fraud susceptibility in vulnerable consumers. *Basic and applied social psychology*, *36*(3), 272-279.

Last, based on what we are seeing in the most recent reporting data, cryptocurrency is playing an outsized role in today's fraud landscape. Consumer fraud thrives in complex environments, and cryptocurrency has created a playground for international scammers.

Ultimately, we need greater investment in fraud detection within the private sector; for companies to be proactive when fraud is suspected instead of reactive when the money is already gone. In addition, consumers need evidence that their complaints are taken seriously by law enforcement and that by reporting, recovery and redress are possible. Only through a coordinated response from policymakers, companies, law enforcement, and consumer protection advocates can we outsmart the criminals who prey on American consumers.

County of San Diego

NICK MACCHIONE, FACHE
AGENCY DIRECTOR

HEALTH AND HUMAN SERVICES AGENCY
AGING & INDEPENDENCE SERVICES
P.O. BOX 23217, MAIL STOP W-433
SAN DIEGO, CA 92193-3217
(858) 495-5885 • FAX (858) 495-5080

KIMBERLY GALLO
DIRECTOR
AGING AND ADULT SERVICES

Testimony before the Senate Special Committee on Aging
September 22nd, 2022
Nancy Pham-Klingler
Senior Adult Protective Service Specialist
Health and Human Services
San Diego County

Good morning, Chairman Bob Casey, Ranking Member Tim Scott, and members of the Committee. My name is Nancy Pham-Klingler, and I am the Senior Adult Protective Service (APS) investigator assigned to the financial fraud unit in San Diego County, California. Thank you for allowing me to join you today to discuss a topic I am passionate about and dedicated to: fighting against fraud and scams.

Over the past year, I have been privileged to be the primary APS investigator attached to the San Diego County Elder Justice Task Force; a partnership of the San Diego County District Attorney's Office, the FBI, local law enforcement in San Diego County and Adult Protective Services seeking to impact scams against older adults.

San Diego County is home to over 3.3 million people. Of that, approximately 680,000 are individuals over 60 years of age. From 2000 to 2030, it is projected that adults 60 and older will increase by 130% while the general population will increase just 38%. That means one in four San Diegans will be age 60 or older.

These numbers are real. Adult Protective Services has witnessed firsthand the increase in APS referrals over the years, particularly cases with a nexus to scams and financial abuse. From June 2021 to July 2022, over 1,200 APS scam-related cases were referred to our office with an estimated loss of over $34 million dollars. It's clear we have an issue. An issue that our most vulnerable population, who have spent years and years of hard work saving for their golden years, only to be deceived and have their life savings stolen under false pretenses by vicious perpetrators.

When responding to these cases, we are the first sign of hope to the victims of these crimes. APS frequently is the first to be there to help them and start the processes to potentially recover their losses, bring some sense of security back, and protect them from future exploitation. During our investigation, we must build a rapport, gain their trust, and assess for safety all while ensuring that we gather all the necessary evidence to bring our cases to the next level. What is the next level, you may ask? As we know, without evidence there is no crime. Our APS team members, along with our local law enforcement agencies in San Diego have been trained to gather key details such as: How did the

scammer contact you? What company did they represent? What account numbers and financial institution(s) were mentioned during your conversation? How was the money sent? What dates and times did the scammers contact you?

These cases are complex. Some top scams we currently see use Mobile Cash Apps, Peer-to-peer money transfer services and social medial engineering. Scammers falsely claim to be a politician seeking donations, work-from-home opportunities to make extra cash, overpayment of an Amazon account, gift cards, and of course Cryptocurrency. How can we confiscate a Bitcoin machine that an elderly person just walked up to and deposited $25,000 in cash with a QR code that they just received via text message?

As difficult as these cases are, recovery of these funds is potentially possible. One example of this is the following case.

On July 13, 2021, San Diego County Adult Protective Services was contacted by San Diego Sheriff's Department with concerns about a possible local Publishing Clearing House (PCH) scam victim. There was a cash package located in Florida that came from a San Diego address. Upon investigating this residence, we located a mailer with our elder's name on it. With the support and assistance of our Elder Justice Task Force, I was able to reach out to appropriate parties to gather necessary information to create an APS referral. I was assigned this case which allowed me to have open communication with the victims identified financial institution, natural support, and local law enforcement. Through collaborative work, I was able to conduct a records request under the Gramm-Leach-Bliley Act (GLBA) (15 U.S.C. §6802I(8); and 15 U.S.C. §6802(e)(3)(B)): and share information with our local law enforcement under California Law, State Welfare and Institutions Code §15610.45. The victim was located, interviewed, and confirmed that she had sent over $215,000 to various individuals through the direction of employees from PCH. One of the payments was to the San Diego address where the package was sent from in Florida. This is not an uncommon method of payment where scammers are using our most vulnerable citizens to launder money for them and ultimately requesting for cash payment to be mailed out to a random address. I worked with the financial institution and reviewed over 271 pages of bank records to confirm that our local victim sent the money to another senior resident and her check was cashed by the receiving senior's bank. Collaborative work, works.

I'm here today speaking to you because this is a national problem crossing state and international borders. In the past year, according to IC3.gov, more than 92,000 victims over the age of 60 reported losses of $1.7 billion, and that is just what has been reported. This represents an increase of 74% from 2020. This is a crisis, and without swift action the trend will continue.

Reporting on elder financial abuse is mandated. We have infrastructure systems in place to report scams; IC3.gov, FTC.gov, FBI.gov, APS, and local law enforcement, but what we need is continuous support and additional resources so agencies involved can help solve the greater issue. That greater issue is legislation and targeted education that makes it harder for these scammers to attack our most precious population in our society and put faith back in our public service system, as well as a means to obtain bank records quickly when it has been determined that a financial institution is the gateway for suspicious transactions. Appropriate funding for training our front line Adult Protective Services social workers to identify and investigate scams is critical.

On behalf of San Diego County I thank you for bringing this critical issue to the forefront, and for your continued work to protect the vulnerable seniors in our community. I welcome any questions the Committee may have.

Aurelia Costigan

Testimony Before the U.S. Senate Special Committee on Aging

September 22, 2022

My name is Aurelia Costigan. I was born in Pittsburgh, Pennsylvania. I was married twice, and both of my husbands have died. I've been widowed since 2008 when my second husband passed. I used to be a school bus driver and also worked in health care for several years. I'm now retired on Social Security and receive Surviving Widow's Benefits. I live in the North Hills of Pittsburgh with my youngest daughter. I have two daughters, three grandkids, and two great grandkids.

Last September, I got a phone call from the number that is listed on the back of my debit card. This man said he was from Dollar Bank and told me that there were two suspicious activity charges on my account from Tennessee. He said one was from a grocery store, and the other from a movie theater. And he asked if I was in Tennessee and made these charges. I said, "No, I live in Pittsburgh. I've never been to Tennessee." He asked if I had any relatives or friends that lived there that could have used my card. I said no. So, he said to prevent having to cancel my card and issue a new one, he could help me with that by adding a Zelle account which would protect my bank account. I don't even know what Zelle is. He said it's something that would protect your account. I said, "Oh that's good."

And then he said, to know that he was actually speaking with Aurelia Costigan, he needed some form of identification to prove that he was actually speaking with Aurelia. He asked if I had an online banking number, but I don't use that. I go into the bank myself personally if I have to do any kind of banking. So, he said the only other option was to use my Social Security Number. I thought that sounded feasible. I assumed he was from my bank. He

called from the right number. So that was the end of the conversation. I said, thank you. We hung up.

And then about 5 to 10 minutes later, my phone starts blowing up. It's notifying me of charge after charge after charge. One after the other. Twenty-two, to be exact. I panicked, went to the bank, and told them about the phone call. And they said, we don't even have any charges from Tennessee on your account. Then that's when I realized it was a scam.

So, they said that they would look into it. The manager of my bank said, "I won't quit until I find that money." I was told to notify the police and file a complaint with the State Attorney's office, both of which I did. The police officer was very helpful and understanding. He provided me with resources and pamphlets. And he even held my hand and said that he really felt for me and other people that are taken advantage of like this. But I was absolutely a wreck. I couldn't sleep. I had trouble eating. I was just devastated. The money I lost - $1,800 – was a lot of money. It takes me a long time to earn money like that. I'm on Social Security, I have to save my money. Because sometimes your car breaks down or a medical expense comes up. Those kinds of things happen, and you need to have some kind of back-up. But I thought I was never going to get that money back.

But thankfully, maybe a month or so later, my bank was able to get my money back – the full $1,800. The State Attorney's office told me that I was very fortunate that my bank worked so hard with Zelle to get my money back. I felt like I could finally calm down again. I had done a lot of praying.

But I know not everyone has that experience. These scammers get away with this every single day. Elderly people like myself, we are always the trusting type of people. But now, I tell

people: don't give absolutely any information about yourself to anyone on the telephone. I tell my friends and family my story as a warning. I tell them to be careful. I hope that we can do something so that this doesn't happen to someone else.

Polly Fehler: Written Testimony
Seneca, South Carolina

U.S. Senate Special Committee on Aging
September 22, 2022

Thank you, Ranking Member Tim Scott and Chairman Casey.

My name is Polly Fehler. I am 76 years old. I am the mother of two sons, grandmother of five, a retired Registered Nurse and RN educator, and a retired United States Air Force officer. My husband of over 48 years died 9 years ago, and I have lived in the same house in Seneca, South Carolina for 32 years. I am here today to tell you about the scam which upended my world last year.

I have always paid my bills on time and managed to pay our house off early. I have worked hard to maintain a lifestyle that has been thrifty, and we taught our sons the same. I pride myself on not spending foolishly and having sharp financial instincts. But when I realized what had happened to me, the bottom didn't just fall out of my life—I'd dropped straight into Hell.

I had been having trouble with my old computer, but it was in the middle of the pandemic, so no one could come over to help nor could I go to my local Staples. The pandemic isolated me completely. In January 2021, I rushed to buy a new computer. Things were going back to normal and I would get my life back!

On April 13, I was using my new laptop on public Wi-Fi and suddenly a pop-up appeared on the home screen; a large blinking orange triangle alerting that my computer had been compromised. Anxious I was going to have computer problems again, I immediately called the listed number on the screen. A reassuring voice alleging to be a representative of Microsoft answered. He told me to buy a protective software for $299, which included computer monitoring for two years, to track issues. I was given a guarantee that he would even call me to check for problems. As far as I could tell, this was great customer service. I got another call on June 14 from the same man who said that he was calling to check on the program. If it was not working, he assured me I would receive a full refund, plus an extra $100 for the inconvenience.

To run a test of the software, I had to give him full access. During this "test," messages flooded the screen. And, there it was again: An alert claiming my computer had been compromised. I told him to send the refund in a check to my home address. He said he couldn't do that because I had paid for the service electronically. He moved to a different browser window and the screen broke out into chaos with numbers and even letters rolling past. Then, suddenly, they stopped. The scammer feigned outrage, saying I intentionally stopped the chaos when my checking account reflected a $20,000 deposit. I couldn't see this alleged number he was talking about. Then, without me even touching my laptop, he opened a window showing my checking account. I was stunned. How in God's name did he get in there? It had a balance of $26,000; $20,000

more than I should have. I became frantic, I had no idea where this money came from and I wanted nothing to do with it. The scammer was furious, demanding that if I didn't give the money back immediately Microsoft would sue me, send me to collections, and ruin my credit. I had worked so hard my entire life to maintain good credit. I was terrified and felt I had no option but to do anything he said.

He told me to wire the $20,000 to a Microsoft subsidiary in Vietnam. The instructions were to tell USAA that I knew this person and owed the $20,000. After I completed the wire transfer, I called USAA to report what had happened. They told me, immediately, I had been scammed. The next day, a fraud investigator called to ask what happened since USAA constantly monitors my banking activity. They could see I had taken out $20,000 on my home equity line of credit, transferred that money to my checking account, and wired it out. I told the truth: I never applied for the credit.

Now, I owed $20,000 with interest. A short time later, I got a notice that the interest was overdue followed by a scary letter saying I qualified for filing bankruptcy. Not having monthly funds to pay, I sold off my Individual Retirement Account (IRA) to not lose my home. The situation snowballed into a hellish nightmare. I tried to find legal advice, any kind of help. I reached out to everyone until I found Diane Lee, an astute local reporter, who told my story and has provided me hope and support.

After suffering through this scam, I was alone and depressed, even losing my spirit to live. For days I sat alone and hated myself for what happened; at times, not getting out of bed. I thought I lost all faith in God. I opted out of all community and church activities, committees, and leadership roles. I couldn't function as the person I had been.

I am here today because I'm a survivor. God is giving me the strength to reclaim my life! I hope we can prevent others from falling into this unmatched misery, saving others from falling into the darkness that comes with losing your self-worth and retirement savings in a click.

Thank you for listening and I look forward to your questions.

Questions for the Record

U.S. Senate Special Committee on Aging
"Stopping Senior Scams: Empowering Communities to Fight Fraud"
September 22, 2022
Questions for the Record
Dr. Marti DeLiema

Senator Mike Braun

Question:

As the criminal enterprise moves hand-in-hand with emergent technology and innovations in the financial sector, bad actors continue to develop new ways to defraud consumers and carry out other illicit financial activities in the rapidly changing digital landscape. Heavy concern rests with the ability of our law enforcement bodies and regulatory agencies within the federal government to effectively prevent and respond to these hi-tech crimes and fraud schemes. How well are relevant federal agencies and enforcement bodies doing in being proactive, as opposed to reactive, in prevention and response measures to new scams and emergent financial crimes targeting consumers, and where can current efforts be focused to better ensure protections for our most vulnerable populations from falling victim to these types of schemes, particularly aging Americans?

Response:

I agree that federal agencies should work toward *proactive* approaches to fraud detection and prevention, especially in the face of emergent money transfer methods that will continue to evolve. Below are several of my personal policy and practice recommendations to ensure early fraud prevention, intervention, and recovery. These represent my own views and options and do not represent any government agency.

- The financial services sector needs to invest more in fraud detection systems and review processes to identify vulnerabilities quickly. We need a dedicated national fraud reporting system for these entities to share time-sensitive information with federal and local law enforcement and Adult Protective Services agencies.

- Federal regulators need to empower financial institutions (perhaps through safe harbor laws) to refuse suspicious transaction requests from customers suspected to be involved in a scam, even if their refusal upsets the customer. Stopping the money before it leaves the customer's account is more effective than attempting to claw it back once it has been stolen.

- A short, temporary delay period in a receiver's ability to access/withdraw funds after a victim sends them money via a person-to-person money transfer or gift card purchase would give consumers a brief but vital window to report fraud and protect their money.

- Nothing is more discouraging to a victim than hearing, "This is out of our jurisdiction." Policing is traditionally based on the location of the crime, the victim, and the offender, but the internet has disrupted policing-as-usual. Scams are a global problem and US federal agencies are

limited in the extent to which they can locate, apprehend, and prosecute international fraud perpetrators. Collaborating with and coordinating investigations and enforcement actions with international law enforcement partners is essential. Working in concert with international agencies could have a substantial impact on decreasing fraud prevalence and achieving justice.

- Those who have had money stolen in a fraud scheme need tax relief, bankruptcy assistance, advocacy to negotiate with banks and creditors, financial counseling, and mental health counseling. These services should be supported using the Crime Victims Fund established through the Victims of Crime Act (VOCA). Currently these funds are not available to most fraud victims.

Question:

Are there opportunities to incentivize collaboration in data and information sharing between agencies, law enforcement, and local organizations to more effectively identify current fraud and scam trends, and detect emergent ones?

Response:

Financial institutions and payment processors have transaction-level data that could provide information on current and emerging fraud trends. They are also motivated to detect and prevent fraud to minimize their exposure to reputational and financial risks. But companies feel encumbered by a myriad of laws designed to safeguard customer and client information by restricting data sharing. Those restrictions, though well intended, give criminals the upper hand. Every minute counts for law enforcement to track and recover stolen funds. Delays in information sharing—between financial institutions and law enforcement, and between the sending and receiving financial institutions—makes it unlikely that funds will be recovered. Restrictions on data sharing may also mean that companies are not alerting federal agencies to trends they are observing in real time.

We need more cross-sector collaboration and data sharing, not only to detect new fraud trends, but also to work existing fraud cases and pursue justice for victims. Open communication channels are critical, and private sector companies—whether they be finanical institutions, payment processors, or technology companies—need to be able to pass on information about emerging vulnerabilities. A body of academic research has shown the value of multidisciplinary teams (MDTs) to address complex healthcare and elder/child abuse cases. We need local and federal MDTs organized around fighting fraud and cybercrime that can overcome communication barriers. Team members could include security experts, financial crimes investigators, police detectives, federal law enforcement, social services workers, and victim advocates. Participants should be authorized to share personally identifiable information on alleged victims and perpetrators when working together on complex cases.

Research indicates that participating on an MDT helps individual team members step outside of their disciplinary bubbles. They begin to understand the roles and capabilities of other professionals and agencies. By engaging in the full process of fraud detection, reporting, investigation, and case resolution, MDT participants can improve their handling of future cases.

I also believe that there needs to be more information sharing in the direction of law enforcement

to financial institutions. Banks and broker-dealers need updates on what actions were taken after they filed a suspicious activity report (SAR) or adult protective services (APS) report, and how they can help safeguard the customer moving forward. When financial institution employees observe their reports going into a black box and receive no communication, they lose the motivation to file comprehensive and timely reports moving forward. Disaffection is incredibly harmful to fraud victims.

U.S. Senate Special Committee on Aging
"Stopping Senior Scams: Empowering Communities to Fight Fraud"
September 22, 2022
Questions for the Record
Ms. Aurelia Costigan

Senator Mike Braun

Question:

Ms. Costigan, as a victim and scam survivor, you know first-hand about the approach and methods used by criminal to target older adults. Given this, I am sure this committee would be well-informed to hear about your insight regarding what information, tools, or educational resources you wish you might have had before your scam crime took place. What could have made the biggest impact for you in terms of education and outreach services on scams and frauds, and how do we best raise awareness for seniors and aging Americans going forward on current methods frequently used by these scammers and criminals?

At this time, responses are not available for printing. Please contact the U.S. Special Committee on Aging for further updates and to perhaps obtain a hard copy, if available.

U.S. Senate Special Committee on Aging
"Stopping Senior Scams: Empowering Communities to Fight Fraud"
September 22, 2022
Questions for the Record
Mrs. Polly Fehler

Senator Mike Braun

1) Mrs. Fehler, as a victim and scam survivor, you know first-hand about the approach and methods used by criminals to target older adults. Given this, I am sure this committee would be well-informed to hear about your insight regarding what information, tools, or educational resources you wish you might have had before your scam crime took place. What could have made the biggest impact for you in terms of education and outreach services on scams and frauds, and how do we best raise awareness for seniors and aging Americans going forward on current methods frequently used by these scammers and criminals?

Polly Fehler's response:

Senator Braun: In response to the above questions, I was the victim of a hacker who claimed to be a Microsoft agent, who gained access to my bank account by logging my computer keystrokes over a period of 2 months without me knowing. The hacker then fraudulently activated my Home Equity Line of Credit (that had a Zero balance - my husband had opened 17 years prior) and withdrew $20,000 and transferred it into my checking account. The hacker then claimed it to be an overpayment of the $399 refund he was supposed to return to me for Microsoft's cancellation of a computer monitoring system he claimed no longer was working. When I testified before the Committee Aging, you heard the story of his clever manipulation as he pressured me to wire money to what I thought was a Microsoft representative in Vietnam. My first four points below address your questions on **what might have helped me before the Fraud and Scam took place**. I have bolded the facts in the explanations below.

(1) The first thing that should have happened was that USAA, with whom I had been a member for over 41 years, needed to notify me that they were activating my **17 year inactive** Home Equity Line of Credit to **see if I had requested** this new **$20,000 loan**. USAA never notified me, not by email, text, or phone. I was not told until the following day, when a Fraud investigator called to inquire about my bank activities. **ALL FINANCIAL INSTITUTIONS SHOULD BE REQUIRED TO NOTIFY THEIR CUSTOMERS WHEN UNUSUAL OR LARGE TRANSFERS OF MONEY ARE TO BE MADE**, before the transfer is completed. The first transfer should never have happened. USAA could have stopped it by questioning me.

(2) I immediately called USAA when I got off the phone with the Fraud and Scam hacker to report what I thought had happened. (I did not even know all that had happened!) The USAA person that took this call should have not only given me the **national Fraud Contact number** the Senate had established, **855-303-9475***, but also other possible fraud support and report people to contact. **All suspected fraud or scam victims should be given this Fraud number. And it should be staffed with people who can make a**

difference to Fraud and Scam victims!

This bank should also have given me an idea about **what was going to happen within the USAA investigation**. All the person I reported to on the phone said was, "An investigator will contact you tomorrow." When I asked when, she said "in the morning". My response was that "this has just happened, can't someone **do something NOW!?**" She just said that no one was in the office now, so nothing would be started. AND this person could have been a little **more** personally **supportive.** She was bland in her responses. I still wonder, would immediate action to the Fraud and Scam by USAA's team been able to stop the money transfer from being completed?

(3) When the fraud investigator did not get back to me first thing in the morning, I called back to the USAA Fraud Line. I was told that when he needed to talk with me, the investigator would call. It was like even though something big was happening to me financially, I was not entitled to know about this investigation. **Fraud teams, keep your customers-victims notified specifically about their situations**.

(4) Finally, and perhaps most importantly, it is crucial to **establish an independent body that scam victims can go to when the same institutions that are involved in the Fraud/Scam (banks and financial institutions) deny victims any compensation**, *even when the victims present* ***evidence that the institution failed to protect them.***

(5) The following are the ways I tried to get help, mostly to no avail, over the next days and weeks and months. **I called:**

A. **USAA regularly,** for months, with questions and to try to find out what was happening with this case. Each time a different staff person answered the phone. I was told that I could not request to talk to any one specific person, that the staff that answered the phones got caught up on my case by the notes the previous staff members made. I probably called USAA about 15-20 times.
   (i) I called in between to ask to **speak to anyone in authority**, to have them contact me at least once with case decisions. No positive response.
   (ii) I was called after reporter Diane Lee got the case reopened, (see below) and was told this was a scam, not fraud, they did not need to hear from me about it again. I requested that the least USAA could do was send me something in writing about their final decision, and about a month later I did get a letter. This was the first and only time I had anything written by USAA.

B. **Federal Trade Commission**, who talked to me for some time and took all my contact information. Staff said they would call me back - no one did. No Senate initiated phone number (855-303-9475*) was given to me.

C. **Seneca Police Department,** who sent a policeman to the house to talk to me. A report was filled out. No resources* recommended.

D. I was told the **Oconee County Sheriff's Dept** did not handle situations like this.

E. **SC State Police Dept.** Told it was beyond their jurisdiction, it was a national Fraud situation. No number* given out.

F. **Several area lawyers**. Each lawyer's staff took my message, what the situation was about, and not one office called me back. No other references* given to me.

G. **SC State's Attorney** staff took my message. No one returned my call. No reference number* given out.

H. **My son**, Timothy Fehler, a Furman University professor. He talked with colleagues about the situation and was given no resources*,
I. **AARP**. This was a very supportive unknown person I talked with. He listened, suggested ways to get through the situation emotionally. The volunteer told me AARP did not have legal references, nor did they give me any numbers to call*. They suggested I call the local Senior Center.
J. **Oconee County Senior Solutions**. The staff there suggested I get ahold of the SC Legal Assistance and gave me their state number. No other numbers* given.
K. **SC Legal Services**. They gave me the number for the SC Upstate Office in Greenville, an hour from me. I called this number at least 10-12 times and left messages before I got a call back telling me that staff answering the phone would forward my call to Attorney Susan Ingles. No other resources* given.
L. **Attorney Susan Ingles.** It took weeks to converse with her, apparently due to her caseload. We finally set up an appointment at her office. My Greenville son went with me but was not allowed entry into building suites due to their remaining Covid-19 restrictions. Told to wait in the small entry area, no seats, he stood there for almost an hour while I talked with the attorney. She told me to forward financial information to her email address and we would progress from there. I did, and she did not get back to me for several months; when she did she said she had been ill. When Attorney Ingles did call, she asked if she could give my phone number to an investigative local TV news reporter for WSPA7, Diane Lee. Hesitantly I agreed, and that is how the Senate aides found my story.
M. **Diane Lee, investigative reporter**, was the most interested in my case. She and I met in person in my home with a camera man. She told me the pros and cons of the situation, since she was deeply involved in research about Fraud and Scams, especially with the elderly in South Carolina. She has continued to maintain contact with me. I allowed her to speak to USAA for me: after some time, Diane Lee got a USAA PR representative to speak with her and reopen the case. But soon after that USAA closed the case. Again, I was not contacted by USAA about the case status; Diane was the person who told me..
N. After the TV segment on Fraud was aired, **SC State Senate President Thomas Alexander's Office** called. He had seen my short segment that Diane Lee included in the TV Fraud and Scam Report. State Senator Alexander attempted intervention in my case, but nothing was successful. His Administrative Secretary, Martha Casto, called to update me several times.

Senator Braun, I was delighted with the interest the Committee on Aging's Senators and staff took in my case. They were extremely supportive, and with their 3-way conversations, convinced me that this was an important issue to share my story and insights. I knew that my USAA case was closed, but have felt that no person should ever have to live through the misery this type of experience caused my life. And millions are still getting hit with the pain, fear, blame and guilt I lived with because this crime is so rampant. Maybe I could make a small difference by warning others. So I came to Washington, DC, and spoke on September 22, 2022! This was a difficult task, but the entire Committee on Aging was so supportive. I got the closure I needed to begin healing. I thank you, your colleagues, and your staff.

On raising awareness: Since the meeting of the Committee on Aging in September, 60 copies (50 English and 10 Spanish) of the book ***Fighting Fraud*** by Senators Robert P. Casey and Tim Scott were sent to me, at my request. Given to Seneca community members, as well as to many church members, friends and family, the book has received acclaim as "helpful, informative, interesting, valuable, shocking". I have gotten calls thanking me for getting a copy to folks. I hope that this book soon becomes a resource available at all Senior Centers in the nation. Actually it has important information in it for all ages! Town and city libraries should also have it in their collections.

Another point I want to make is that the Reporting Fraud/Scam **phone number 855-303-9475* should be publicized.** It should be listed as a resource in phone books, within organizations, in advertisements, in newspapers and magazines, on educational TV ads. All mental health and medical counselors, teachers, police, etc. in the US should be given this resource. It needs to become known by people. Being alone in this sea of scam artists is so debilitating, and it does not have to be that way. This is a world-wide disaster hitting hundreds of thousands.

Another thing, the **scammers need to be severely punished** and publicly humiliated. Crimes like these do not hit merely one class of people, but us all. **Coordination of information needs to be done among organizations and countries** so we can identify those responsible and start putting an end to this. The Fraud and Scam crime is growing!

I feel that **raising the awareness** can be aided by **use of our televisions and movie outlets**. A couple of well-done and interesting documentaries, and then the advertisement of these, would be helpful. Movies showing the scammers as the monsters they are would help, too. Getting the public **involved in understanding** the huge loss and suffering it's causing can help prevent it.

Dear Senator Braun, now I have completed this long response, I must share **what happened just last night.** I received a **phone call from USAA** telling me that my USAA Fraud and Scam case was reopened, and it was decided by their banking fraud committee that **USAA will be refunding me**. What a Christmas surprise and gift, though I do feel the refund was warranted.

Then today, just as I was wondering if that phone call was but yet another scam, a **letter** was in my USAA account this morning **titled *FRAUD CLAIM RESOLVED IN YOUR FAVOR***. The letter stated **$21,613.28 was being credited to my USAA account**. Payee is *International Wire Transfer*. It really is happening! God has blessed me beyond expectation.

I feel **I have Investigative Reporter Diane Lee to thank for initiating the attention to this crime with her honest TV report, as well as supporting me so completely for almost a year. And then I have the Committee on Aging to thank, for I do not feel that this fraud would have been recognized by USAA without my being asked to testify before this committee in Washington, DC, on that scary day in September 2022. The US Senate Committee on Aging and its staff have been deftly responsive to an old lady's needs. Senator Robert Casey, Chairman, and Senator Tim Scott, Ranking Member, and working committee: ya'll rock!**

I offer my humble gratitude to those who made this happen, in all ways, big and small.

Polly Fehler (pollyfehler@gmail.com)

Polly D. Fehler

cc: Sen. Robert Casey
Sen. Tim Scott
Sen. Mike Braun
Aide Francisco Flores-Piovrat

USAA Federal Savings Bank
10750 McDermott Freeway
San Antonio, Texas 78288-0544

FRAUD CLAIM RESOLVED IN YOUR FAVOR

POLLY D FEHLER
[redacted]

December 22, 2022

Dear Captain Fehler,

USAA is committed to providing excellent service and delivering on our mission to facilitate your financial security. We appreciate your patience as we investigated this matter for you. As a result of our investigation, a credit titled "Fraud Credit" in the amount of $21,613.28 was issued December 22, 2022 for the following transaction or transactions:

Account ending in:	[redacted]
Claim date:	November 3, 2021
Total claim amount:	$21,613.28
Total amount credited:	$21,613.28
Payee name:	INTERNATIONAL WIRE TRANSFER
Transaction date:	June 14, 2022
Transaction amount:	$21,613.28
Amount credited:	$21,613.28

If it is determined that the transaction is valid, or if we recover some or all of the funds, we reserve the right to reverse the fraud credit. We will notify you before we reverse the fraud credit and any applicable interest earned.

Please retain this letter for your records and provide, if necessary, to any merchants or other financial institutions who assessed fees related to the disputed transaction.

As always, we value your business and the opportunity to serve all your financial needs.

Sincerely,

Stacey Nash
Senior Vice President & General Manager, Bank Fraud Management & Central Operations
USAA Federal Savings Bank

Statements for the Record

Statement for the Record

On Behalf of the

American Bankers Association

Before the

Special Committee on Aging

of the

United States Senate

September 22, 2022

Statement for the Record

On Behalf of the

American Bankers Association

Before the

Special Committee on Aging

of the

United States Senate

September 22, 2022

Chairman Casey, Ranking Member Scott, and distinguished Members of the Committee, the American Bankers Association[1] (ABA) appreciates the opportunity to submit a statement for the record regarding the hearing titled, "Stopping Senior Scams: Empowering Communities to Fight Fraud."

Over the past several years, there has been an increasing trend in criminal activity targeting America's seniors. With the onset of the COVID-19 pandemic, financial fraud became more pronounced as a result of isolation from lockdowns and social distancing. Scammers capitalized on societal disruptions and are using a variety of tactics to manipulate and victimize seniors. They may go door-to-door or utilize social engineering techniques, phone calls, texts, emails, social media, and other approaches to steal seniors' financial assets and identities.

Given the circumstances seniors are facing, ABA, its non-profit foundation, and the banking industry are expanding their commitment to protecting America's elders and are taking specific steps to combat elder financial exploitation.

Background

Often referred to as the "age wave," the United States is in the midst of a demographic transition. Ten thousand Baby Boomers[2] are turning 65 every day and will continue to do so until 2030 – at which point 20 percent of the nation will be of "retirement age." Just four years later, by 2034, there will be more people aged 65 and older than children for the first time in our nation's history.[3] This shift is affecting people and industries alike throughout the country, and the financial services sector is no exception.

---

[1] The American Bankers Association is the voice of the nation's $23.7 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2 million people, safeguard $19.6 trillion in deposits and extend $11.8 trillion in loans.

[2] Defined by the U.S. Census Bureau as people born between 1946 and 1964.

[3] https://www.census.gov/newsroom/press-releases/2018/cb18-41-population-projections.html.

Older people tend to have more wealth than their younger counterparts. The most recent Federal Reserve Survey of Consumer Finances notes that the median net worth of people under 35 is $13,900, while the median net worth of people aged 65-74 is nearly 20 times that at $266,400.[4] This fact is one of the reasons that elders are attractive targets for fraudsters.

Each year, older Americans lose billions of dollars to financial exploitation. Citing exact losses is difficult as older adults are often reluctant to report abuse. According to the New York State Elder Abuse Prevalence Study, only 1 in 44 cases is typically reported.[5] However, the Financial Crimes Enforcement Network indicates that financial exploitation "affects at least 10 percent of older adults each year,"[6] while AARP reports that average losses are as high as $120,000 per victim.[7]

Losses from such abuse are significant and take an emotional toll on top of the financial impact. Victims often become depressed and experience intense feelings of shame as well as fear. Many lose their savings, while others may also lose their homes and suffer greater risks of mortality, [8] harming one of America's most vulnerable populations.

Recognizing the challenges facing America's older population, both ABA and the banking industry take protecting older customers seriously and are actively working to safeguard seniors and combat elder financial exploitation.

American Bankers Association Efforts to Protect Seniors

Given the seriousness of the issues facing older customers, ABA works through its non-profit foundation to ensure that all banks, irrespective of membership status, can access tools and resources to prevent, detect, and combat elder financial exploitation. ABA and the ABA Foundation utilize a multi-pronged approach, involving education, partnerships, research, and training to stem abuse.

Education

The ABA Foundation offers banks a free toolkit on "Protecting the Financial Security of Older Americans." This three-part resource is designed to help banks develop a framework on educating and engaging their communities on preventing elder financial exploitation.

Since 2016, 1600 banks have participated in the ABA Foundation's Safe Banking for Seniors program.[9] Through the free initiative, participating banks have access to turnkey materials to inform their communities about avoiding scams, choosing

---

[4] https://www.federalreserve.gov/publications/files/scf20.pdf
[5] https://ocfs.ny.gov/reports/aps/Under-the-Radar-2011May12.pdf
[6] https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf
[7] https://www.aarp.org/ppi/info-2020/the-thief-who-knows-you-the-cost-of-elder-exploitation-examined.html
[8] https://www.sec.gov/files/elder-financial-exploitation.pdf
[9] https://www.aba.com/seniors

executors, financial caregiving, preventing identity theft, and understanding powers of attorney. Banks use the materials to help empower their communities and lead a combination of in-person and virtual workshops, post videos and other content on social media, and share vital information during one-on-one conversations at teller stations. Recent program additions include videos on how scammers target seniors, family imposter scams, government imposter scams, lottery scams, money mule scams, sweetheart scams, and tech support scams.[10] All of the resources are available at no cost to both ABA member and non-member banks.

Through a partnership with the Federal Trade Commission, the ABA Foundation also developed infographics to raise awareness about scams that disproportionately affect older customers. Banks and non-banks alike can freely access and disseminate materials on: Fake Check Scams, Government Imposter Scams, Imposter Scams, Money Mule Scams, Online Dating Scams, and Phishing Scams.[11]

While not targeted exclusively to seniors, ABA's award-winning #BanksNeverAskThat anti-phishing campaign provides real-world tips for consumers on how to identify common phishing scams and protect themselves.[12] More than 2000 banks across the country have participated in the industry-wide campaign since its launch in 2019. The latest iteration launches in October 2022.

Partnerships

The ABA Foundation participates on the National Adult Protective Services Association's (NAPSA) Financial Exploitation Advisory Board (FEAB) to support efforts to encourage and improve collaboration and communication between banks and adult protective services in combating financial exploitation.

The ABA Foundation also partners with the National Sheriffs Association in supporting efforts to train sheriffs' offices around the country about the most prevalent scams against seniors.

ABA works closely with 51 state banker associations from the 50 states and Puerto Rico to provide training and resources to their banking members on protecting seniors. Sample collaborations include joint efforts with the Maryland Bankers Association, Michigan Bankers Association, and the Virginia Bankers Association to create elder financial exploitation prevention summits for bank members.

The ABA has partnered with the National Cybersecurity Alliance[13] for many years on efforts to educate consumers on safe computing practices as part of the annual National Cybersecurity Awareness Month observance, which is held each October.

---

[10] https://www.aba.com/about-us/press-room/press-releases/raise-awareness-on-senior-scams
[11] https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money
[12] https://www.banksneveraskthat.com/
[13] https://staysafeonline.org/

ABA also supports the U.S. Department of Justice's annual Money Mule Initiative (MMI) to raise awareness about money mule scams.

Research
Since 2017, the ABA Foundation has conducted three biennial Older Americans Benchmarking Surveys to understand the latest products and services banks offer older customers, the training they offer staff on identifying elder financial exploitation, and how banks are educating their older customers about safeguarding their financial assets and identities.[14]

Training
ABA offers an online module on elder financial exploitation prevention through our Frontline Compliance Training program.[15] The course teaches bankers about how to identify elder financial exploitation, understand how seniors are vulnerable to financial exploitation, and the role banks play in recognizing and reporting signs of exploitation. Annually, more than 50,000 bankers take the course.

The ABA Foundation developed a resource titled, "Protecting Seniors: A Bank Resource Guide for Partnering with Law Enforcement and Adult Protective Services."[16] It provides banks with key information on financial scams, observing changes in consumer activity, the roles of adult protective services and law enforcement in combating senior scams, and ways to collaborate with community partners.

Each year, in collaboration with the American Bar Association, the ABA hosts a dedicated panel on elder financial exploitation through the ABA/ABA Financial Crimes Enforcement Conference. Panelists generally include bank regulators, banking professionals, law enforcement, federal agents, and others who speak about ways to effectively combat elder scams and fraud.

Since the onset of the COVID-19 pandemic, ABA created the Senior Protection Taskforce, a forum open to all member banks to discuss challenges and best practices in combatting scams and protecting older customers. Bankers meet virtually three times a year to assess trends, compare notes, and learn from each other.

Additionally, the ABA Foundation hosts several free webinars for the banking industry on a variety of topics relating to safeguarding seniors, including identifying scams, bank partnerships to protect elders, caregiver support, cognitive decline, as well as tackling money mules, among other subjects.

---

[14] https://www.aba.com/news-research/research-analysis/older-americans-benchmarking-report
[15] https://www.aba.com/training-events/online-training/elder-financial-exploitation
[16] https://www.aba.com/-/media/documents/about/foundation/protecting-seniors-partnership-guide.pdf?rev=4a5f4507c56741d3a582cbe7199c4930

Banking Our Nation's Seniors

Older customers comprise the bulk of bank depositors and hold the lion's share of bank deposit balances. As such, banks of all sizes and charters are dedicated to supporting their older customers and safeguarding them from scams. Banks utilize several strategies to protect their customers and communities, including:

Account Monitoring
Banks assign staff to review accounts of older customers when they suspect potential exploitation, flag affected accounts, utilize automated tools and algorithms to monitor and detect unusual activity, and may also open new accounts after closing affected ones for victimized customers. Banks are also increasingly working with fintech companies such as Carefull[17] and EverSafe[18] to incorporate artificial intelligence in their arsenal of fraud prevention tools to mitigate against elder financial exploitation.

Advocacy
Banks have been working with their state bankers associations to enact state laws that allow for greater communication and information sharing with adult protective services and permit delaying transactions when they suspect financial exploitation. Examples include:

- New Hampshire Senate Bill 385, which allows banks to delay transactions to help combat financial exploitation.[19]
- Maryland Senate Bill 175, which requires financial institutions to disclose financial records to adult protective services when investigating cases of financial exploitation.[20] This requirement removes any potential legal ramifications against banks for sharing customer information.

Consumer Outreach & Education
Banks recognize that education plays a significant role in understanding how criminals target seniors. Accordingly, banks of all sizes engage in a variety of consumer outreach and education efforts to inform their communities. Some examples include:

- Large Banks
    - Bank of America offers the Security Center as a dedicated web resource with tools and tips consumers can take to help protect their personal and financial information from fraud, learn about red flags, and how to avoid scams. Bank of America also offers the Better Money Habits™ program, which is a free financial education resource dedicated to helping people

[17] https://www.getcarefull.com/
[18] https://www.eversafe.com/
[19] http://www.gencourt.state.nh.us/bill_status/pdf.aspx?id=31799&q=billVersion
[20] https://legiscan.com/MD/bill/SB175/2022

manage their money, and includes specific information on financial caregiving, privacy, and security.
  - Citi, in partnership with the ABA Foundation, has galvanized a national cadre of bank volunteers to lead Safe Banking for Seniors presentations in communities across the country.
  - JPMorgan Chase, in collaboration with AARP, was the first large bank to train all of its retail branch bankers with AARP's BankSafe training program, helping bankers spot scams and teaching them how to talk to older customers about banking safely. Using the Consumer Financial Protection Bureau's Money Smart for Older Adults, Chase also leads educational workshops in retirement communities, branches, and other locations to inform seniors about how they can protect their financial assets.
  - Wells Fargo instituted an Elder Client Initiative to help coordinate internal stakeholders and educate older customers as well as their families about preventing scams and financial abuse. Wells Fargo offers a free "Hands on Banking" program that includes information tailored to help seniors manage their money safely.

- Regional Banks
  - MidFirst Bank's "MoneyMoments" financial education program supports financial literacy among people of all ages. As part of the program, their team of bank educators lead movie-themed fraud prevention workshops and distribute senior fraud crossword puzzles to area senior centers to help seniors prevent victimization. To creatively reach seniors, they printed a fraud infographic in a local senior journal and their fraud director has served as a guest host on a senior radio station to discuss scams.
  - Old National Bank created the "Money Safety for Seniors" program to enable anyone in the bank's footprint to freely request and participate in a class on how to detect, protect against, and report financial exploitation of seniors.
  - U.S. Bank offers a collection of educational articles and videos that elders and their loved ones can access to learn strategies for protecting themselves and their assets from financial exploitation. The free content includes tips to help people recognize and report common financial scams, stay safe online, and have conversations about financial caregiving with loved ones.

- Community Banks
  - Amboy Bank created the "Protecting Our Seniors" program, focused on educating seniors in the community about identity theft and financial exploitation. Through the program, they share content via bank mailings, posters, seminars, and a dedicated Senior Safety webpage housed on the bank's website.
  - Bank of the Rockies instituted the Senior Champions program at bank branches. Within each branch, the Champions facilitate outreach events to

educate seniors about scams, take targeted approaches to connect with socially isolated seniors, and engage elder justice community stakeholders to help protect older people in the bank's footprint.
- First Community Bank partners with the Senior Housing Crime Prevention Foundation to support the Senior Crimestoppers program and leads educational sessions, such as "Cyber Savvy Seniors" to educate older people in the community.
- Somerset Trust Company hosts financial literacy and fraud seminars throughout the bank's footprint to help people identify scams against seniors. The bank also participates in an annual Elder Justice Day seminar with the local Area Agency on Aging and the Pennsylvania Link to educate seniors and caregivers about avoiding financial scams and accessing victim services.

Training
In addition to required fraud prevention training, banks typically offer additional elder financial exploitation prevention training for their frontline staff. According to the ABA Foundation's 2021 Older Americans Benchmarking Survey, 99% of bank respondents indicated that they offer elder financial exploitation prevention training on how to detect, prevent and report financial exploitation for their customer service representatives. More than eight in ten respondents provide the training at least once a year. Some banks, such as Incredible Bank based in Wausau, WI also provide Dementia Friendly Training to inform bankers how dementia impacts customers' financial security.

Recommendation

The United States would benefit from a national reporting system that would allow all financial institutions to easily report suspected elder financial exploitation into one central location. This system should be accessible to law enforcement, adult protective services, and banking supervisors to access details and request records to appropriately investigate cases while ensuring that the privacy and data security of affected seniors is protected. Such a system would minimize reporting delays that result from individual state requirements and reporting challenges that national and regional banks often experience when working across multiple state lines. Time is often of the essence to stop or thwart financial exploitation.

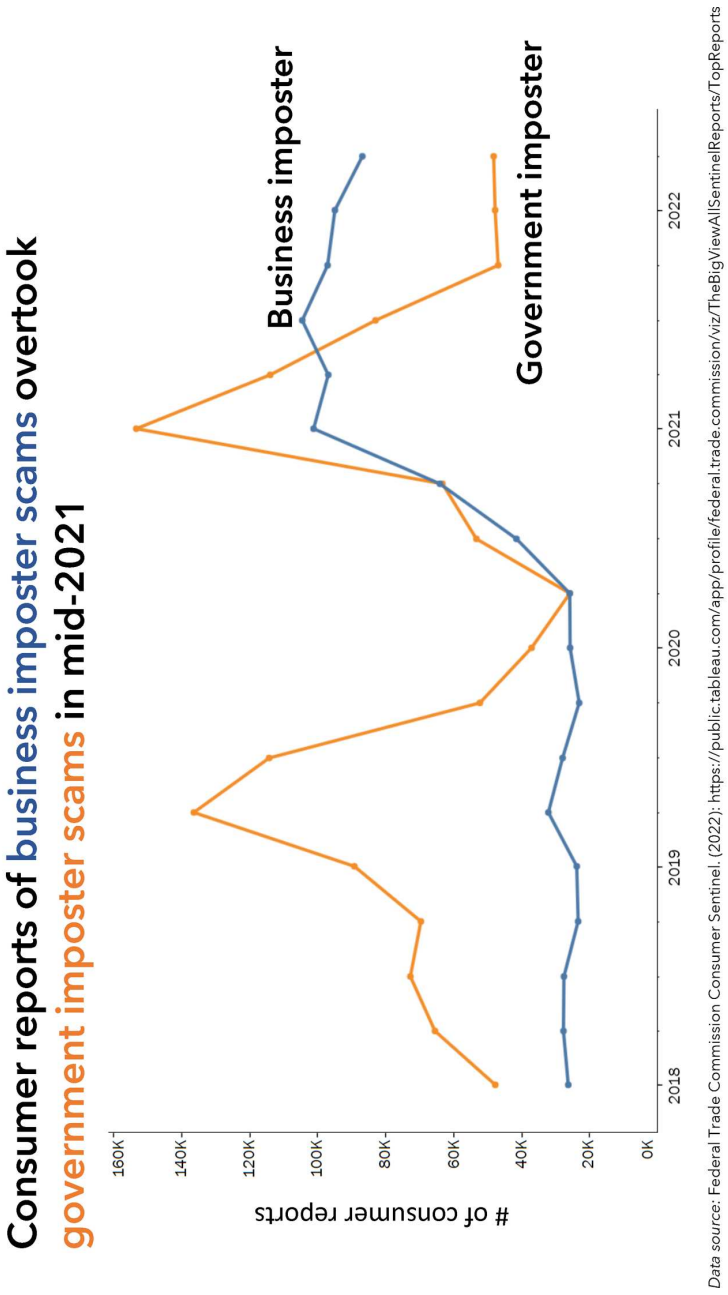
At the same time, it is important for financial institutions to be protected from liability and any system developed should include "Safe Harbor" protections for financial institutions when sharing customer information with law enforcement, adult protective services, and other appropriate government officials regarding suspected elder fraud exploitation.

Conclusion

ABA and America's banks are committed to protecting older customers. We appreciate the Committee's decision to examine scams and abuses facing our nation's seniors.

ABA and its members are available as a resource as you work to support America's elders across the nation.

Dr. Marti DeLiema (slide 1)



Dr. Marti DeLiema (slide 2)