S. HRG. 115–671

STOPPING SENIOR SCAMS

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING

UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

WASHINGTON, DC

MARCH 7, 2018

Serial No. 115–15

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
35–279 PDF WASHINGTON : 2019

SPECIAL COMMITTEE ON AGING

SUSAN M. COLLINS, Maine, *Chairman*

ORRIN G. HATCH, Utah
JEFF FLAKE, Arizona
TIM SCOTT, South Carolina
THOM TILLIS, North Carolina
BOB CORKER, Tennessee
RICHARD BURR, North Carolina
MARCO RUBIO, Florida
DEB FISCHER, Nebraska

ROBERT P. CASEY, JR., Pennsylvania
BILL NELSON, Florida
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
JOE DONNELLY, Indiana
ELIZABETH WARREN, Massachusetts
CATHERINE CORTEZ MASTO, Nevada
DOUG JONES, Alabama

KEVIN KELLEY, *Majority Staff Director*
KATE MEVIS, *Minority Staff Director*

CONTENTS

STOPPING SENIOR SCAMS

WEDNESDAY, MARCH 7, 2018

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

The Committee met, pursuant to notice, at 1:01 p.m., in room SD–562, Dirksen Senate Office Building, Hon. Susan M. Collins (Chairman of the Committee) presiding.

Present: Senators Collins, Fischer, Casey, Gillibrand, Blumenthal, Donnelly, and Cortez Masto.

OPENING STATEMENT OF SENATOR SUSAN M. COLLINS, CHAIRMAN

The CHAIRMAN. The hearing will come to order.

Good afternoon. This Committee's ongoing commitment to fighting fraud against older Americans is raising awareness and making a real difference. Just 2 weeks ago, the Department of Justice announced the largest coordinated, nationwide sweep of elder fraud cases in our history. Involving more than 250 defendants who victimized more than 1 million Americans, the elder fraud schemes charged in this effort caused losses of more than half a billion dollars.

The criminal, civil, and forfeiture cases stemming from this sweep are related to a variety of fraud schemes, ranging from mass mailings, telemarketing, and investment frauds to incidents of identity theft and abuse by guardians. In his remarks, Attorney General Sessions thanked the Aging Committee for our longstanding work to shed light on the widespread issue of fraud targeting our seniors. While important progress is being made, we must not let up on our efforts to educate seniors, their families, and their caregivers about these scams.

The stakes are extremely high. According to the Government Accountability Office, America's seniors lose a staggering $2.9 billion a year to an ever-growing array of financial exploitation schemes and scams. In Maine—the state with the oldest population by median age—about 33,000 seniors each and every year are the victims of some kind of elder abuse, ranging from financial fraud to physical abuse and neglect.

Today our Committee is releasing its updated Fraud Book for 2018. This book, like the ones we have published in the past, lists the 10 most prevalent scams that are reported to our Committee's Fraud Hotline. Our investigators on our Fraud Hotline received more than 1,400 calls from residents from all over the country last year. But once again, a familiar scam tops the list.

For the past 3 years, the IRS impersonation scam has been the most consistently reported to our hotline. In this scam, a con artist pretending to represent the IRS calls demanding money for supposedly past due taxes. The criminals often demand payment in the form of gift cards, and they threaten their victims with arrest if they do not pay up immediately. In this scam, fraudsters use fear to threaten their victims and steal their money.

The perpetrators of the IRS scam are sophisticated and ruthless. They often "spoof" the telephone number so that the caller ID reads the "Department of Treasury" or the "Internal Revenue Service," ensuring that the recipient of the call will answer it. And if the victim does not agree to pay up the money, then the next call often will appear to be from the local police department threatening to arrest the senior immediately.

Other scams on our top ten list include robocalls, lottery scams, grandparent scams, computer tech support scams, romance scams, and elder financial abuse—to name just a few.

Our hotline not only has helped us identify the most common scams but also in some cases to stop them in their tracks. For example, as a result of a tip that came into our hotline in 2016, the Treasury Inspector General for Tax Administration arrested five individuals in connection with the IRS impersonation scam. The Inspector General's investigation ultimately led to the identification and indictment of an additional ten suspects related to this case last year. The IG believes that these 15 individuals victimized nearly 8,000 people and stole approximately $9 million from unsuspecting Americans.

In a similar but unrelated case, 56 individuals and 5 call centers in India were indicted in October 2016 for their involvement in the IRS impersonation scam. The Committee's own data show that these arrests had a real impact. Prior to the arrests, nearly three out of every four calls to our hotline involved the IRS impersonation scam. In the 3 months after the arrests, reports of the scam dropped by an incredible 94 percent. Moreover, in 2017, the Committee saw an overall 77 percent reduction in the number of IRS impersonation scams reported to our hotline compared to the previous year. Clearly, law enforcement actions serve as a deterrent to scammers. And that is why I am so pleased that the Department of Justice is now focusing on this issue, making it a priority, and asking the U.S. Attorney's Office to designate an individual who will be in charge of going after scams that are targeting our seniors. Nevertheless, I have to report to you that the IRS scheme remains the most persistent scam reported, and we always see a peak during tax season.

In a more recent case, last month, a woman from Alabama contacted our Committee's hotline to report that her 60-year-old mother-in-law had become the victim of an online romance scam. The woman told us that this con artist, pretending to love her mother-in-law, told her that he wanted to marry her and had her open a joint checking account in both their names. She wanted to deposit her retirement savings into the account because the scammer told her that he would also deposit $23,000 into it. Furthermore, the victim purchased a plane ticket to Nigeria and was scheduled to

depart on February 19th so that she could be with this man who supposedly loved her.

Fearing that her mother-in-law would get on the plane and that she would never see her again, this woman contacted our Committee's hotline seeking assistance. Fraud Hotline investigators contacted the Department of Homeland Security and asked that they intervene. Agents quickly reached out to both the caller and the victim and provided information on a variety of scams including romance scams, Nigerian scams, and scams that trick seniors into being, without their knowledge, international drug smugglers. After speaking with the Homeland Security officials, the victim understood that she was being drawn in to this scheme and she agreed not to fly to Nigeria.

As our 2018 Fraud Book makes clear, while we are making progress, far too many victims are still losing money and, far too often, their entire retirement savings. Law enforcement, consumer protection groups, the AARP, Area Agencies on Aging, and financial institutions play vital roles, but alert citizens are our first and best line of defense.

Today we will hear about innovative ways to increase the public's awareness of these scams, and I am particularly pleased to welcome two of my constituents, Stephen and Rita Shiman, from Saco, Maine. They are going to tell us about their own experience with a common scam, the grandparent scam, and I so appreciate their willingness to speak out because by their coming forward, they will help others to prevent them from becoming victims themselves.

I am very proud of our work in exposing scams that are targeting our seniors. The more that seniors know about these scams, the less likely they are to fall victim. And we give many examples of common scams, as well as tips for how to avoid becoming a victim.

I want to end by saying that we are dedicated to helping our older Americans become more aware and better informed, but this can happen to anyone of any age, and I think it is important that we acknowledge that as well. We are putting the criminals on notice that they will be stopped and they will be brought to justice.

Thank you, and I would now like to turn to Senator Casey for his opening statement.

OPENING STATEMENT OF SENATOR ROBERT P. CASEY, JR., RANKING MEMBER

Senator CASEY. Chairman Collins, thank you very much for holding this hearing, and thank you for your great work on this over many years and the intensity and passion you bring to this subject.

So many experts from around the country have struggled to estimate, just to estimate the total financial impact of scams and abuses that target our seniors, mainly because it is so underreported. However, they know it adds up to at least $3 billion a year in lost savings—and potentially billions more.

The impact of scams on older adults can have dire consequences, and that is probably an understatement. For many seniors, their nest egg may represent a significant source of their monthly income, allowing them to afford rent, health care, and food. Once their funds are stolen, they often never receive adequate reimbursement for that loss.

Last summer, the Lebanon Daily News in Lebanon, Pennsylvania, right in the middle of our state, reported on an 82-year-old Pennsylvanian who lost $30,000 to scammers because he believed he was prepaying the tax on a $10.5 million sweepstakes win. He will never see those winnings nor his $30,000 again. It is our sacred responsibility to take aggressive action, as Senator Collins just outlined, so that not one more senior loses one more penny. That has to be the goal, the ultimate objective.

Today we will hear about the efforts of volunteers and organizations from coast to coast who educate seniors about the slimy tactics that these con artists apply. Helping older Americans and older Pennsylvanians protect themselves and their hard-earned savings is the very least that we can do here in Washington. But the responsibility to protect oneself from a scammer should not sit solely with our aging loved ones.

That is why I am pleased that last year the Federal Communications Commission heeded calls from this Committee to finalize rules that would help stop an illegal call from a scammer before it is even dialed. I am hopeful that industry will use this new tool to take aggressive action against robocalls.

It is why we will also continue to ensure law enforcement has the resources necessary to punish those perpetrating these horrible crimes or knowingly allowing these scammers to receive "payments." And it is why we must continue to work with retailers, pharmacies, banks, money-transferring companies, and the gift card industry to prevent assets from ever leaving the hands of unsuspecting victims in the first place.

I am pleased that we have a Pennsylvanian here to testify today. Mary Bach is our witness, and Mary should not have to drive one more mile to spread the word about scams and con artists to her peers. And I know that Mary is anxious to testify based upon my short conversation earlier, but I still have to introduce you in a few moments. So, Mary, we are grateful you are here, grateful to our other witnesses who traveled here to be with us to give their testimony, and, of course, grateful to our Chairman for holding the hearing.

Thank you.

The CHAIRMAN. Thank you very much.

I want to welcome Senator Fischer and Senator Cortez Masto for joining us also today as we explore this important issue.

We will now turn to our panel of witnesses. First, let me say again how delighted I am to welcome two of my constituents, Stephen and Rita Shiman, from Saco, Maine. Like far too many seniors, Stephen and Rita fell victim to the notorious grandparent scam, which they will describe today. And I am certain that their story will help to prevent others from being scammed.

We will then hear from Doug Shadel, who serves as Washington State director for AARP. AARP has worked so closely with us in helping to distribute last year's Fraud Book, and I am sure that they will this year as well, as we join common cause in helping to educate seniors about common frauds and what they can do to avoid becoming victim.

Ranking Member Casey will now introduce our next witness.

Senator CASEY. Thanks very much.

As I alluded to just a couple minutes ago, I am pleased to introduce Mary Bach. Mary is from Murrysville, Pennsylvania, Westmoreland County, way out in southwestern Pennsylvania, and we are grateful she is with us today. Mary has volunteered with AARP Pennsylvania for 20 years as the chair of their Consumer Issues Task Force. In this role, Mary travels about 15,000 miles a year in Pennsylvania, giving more than 100 presentations to groups and organizations.

Mary, I thought I traveled a lot in Pennsylvania. I think you have me beat.

She has won numerous recognitions and honors, including the Andrus Award for Community Service from AARP, just to name but one. Mary will tell us about the most effective ways she finds to educate seniors about scams.

I also want to recognize her husband, Len, who is here, and I am grateful for his presence and helping to get Mary here today. And, Mary, we are grateful that you are here, grateful for your testimony, and we look forward to hearing your testimony.

Thank you.

The CHAIRMAN. Thank you.

And, finally, we will hear from Adrienne Omansky. She is the founder of the Stop Senior Scams Acting Program in Los Angeles. Ms. Omansky will describe her program's unique model of seniors using theater to warn their peers about scams.

So I want to thank all of our witnesses for being with us, and we are going to start with Mr. and Mrs. Shiman. Thank you.

STATEMENT OF RITA AND STEPHEN SHIMAN, GRANDPARENT SCAM VICTIMS, SACO, MAINE

Mrs. SHIMAN. Good afternoon. I want to thank Senator Collins and the Committee for their interest and work on this problem of scamming of senior citizens. We also want to thank our friend Bill King, the sheriff of York County in Maine, for his work in educating seniors about scamming.

When my husband and I realized we were scammed, we felt so embarrassed and humiliated, we told no one about it except our children and Sheriff King. When we were getting ready to leave for Washington, we had to tell our friends why we were coming. They responded almost unanimously that they either knew someone or had a relative who had been scammed. And so we feel especially pleased to be able to be here because now we feel we can really open up and talk about it, because I think so many more people want to talk about it but are afraid to do so.

There is a special bond between grandparents and their grandchildren. The scammers know this well, and they take full advantage of it. They know that when a child is in trouble, grandparents go all out to help. There was also a concern on our part because of potential racial bias against Kabo, our grandson, who is an adopted native of Botswana.

On the morning of May 28, 2015, I answered the phone and spoke to someone who said he was Kabo. The voice sounded just like him. He said he was in Atlanta, Georgia, and that he had been arrested and was in a county jail. He needed bail money. I asked him what brought him to Georgia from his home in Maryland. He

said a college classmate had died of cancer, and several friends drove to Georgia for the funeral.

Kabo told me he was assigned a public defender who promised him he would be freed upon payment of bond satisfactory to a judge. He was turning to us because he did not want his parents—my son and his wife—to know. He made me promise I would not tell anyone about this. He said the public defender would call us shortly.

The supposed public defender, identified as George Diaz, did call us and said he was meeting with the judge shortly. There was a sense of urgency. If we paid $1,230, the judge would release Kabo. He said the transaction had to be in cash and sent via Western Union to his contact in the Dominican Republic, and he gave us the details. That statement alone should have raised a red flag, but we were so caught up in the moment that we were simply acting on autopilot. He also said that if Western Union questioned this transaction, we should say nothing. He said they legally have no right to ask. As it turned out, no one raised an eyebrow. And my husband will take it from there.

Mr. SHIMAN. When we made payment and nobody said anything, we came home, but it did not take long for us to say, "Something is wrong here." And I got on the phone and called the public defender's office in Atlanta. They never heard of George Diaz, no such person as identified by them. And I knew right away this is totally false. There is nothing true about it.

And then we got really adventuresome, and we did what we should have done to begin with, and we called my son's house. And who picks up the phone but my grandson, Kabo. He says, "I just got out of the shower, and I have been here all along." And I can tell you I was, even with the parting of the money that we had lost, a very happy guy to know this is just a total fabrication.

It is very easy to play Monday morning quarterback. There were so many things that we should have known. We went over this incident over and over again, and we could not believe that we were so duped. We like to think we are sophisticated people, but when it comes to these emotional responses to people that we love, our reason went out the window. And, hopefully, through the work of this Committee and as I have learned so much about AARP and the wonderful work they are doing, we can find ways to constructively prevent other people from becoming victims of this kind of malicious activity.

We really appreciate the opportunity to speak to you today. Thank you.

The CHAIRMAN. Thank you very much for your very compelling testimony. Again, let me express my appreciation, which I know is shared by colleagues, for your willingness to come forward.

I am going to tell my own story about a similar experience a little later, but let us go on to our next witness, Mr. Shadel.

STATEMENT OF DOUG SHADEL, PH.D., STATE DIRECTOR, AARP WASHINGTON

Mr. SHADEL. Thank you, Chairman Collins, Ranking Member Casey, and Committee members, for the opportunity to talk about the current state of consumer fraud that targets older persons. My

name is Doug Shadel, and I am the director of AARP Washington. I have spent a couple decades now both as a fraud investigator and educator and more recently as a researcher trying to understand this crime.

Today imposter scams are on the rise, as we have already heard from you, Chairman Collins. The Federal Trade Commission reports that imposter fraud complaints have risen from about 120,000 in 2013 to over 380,000 in 2017 in the latest Consumer Sentinel report. We did a study at AARP Washington identifying the following top scams, and some of this is repetitive from what you were saying, Senator Collins, but let me just describe a couple of these.

The tech support scam is the No. 1 scam that we see going on that targets our folks. A computer pop-up alert prompts a call to a toll-free number to eliminate a virus, and the scammer charges a fee to remove a non-existent problem.

Phishing scams are a close second behind it. Phishing, P-H-I-S-H-I-N-G. You receive a notice that looks like it is from your bank or credit card company urging you to contact them with personal information to fix a problem with your account, with the goal of stealing your identity.

Close behind that, lottery scams. Someone contacts you to announce you have a won a lottery and all you need to do to claim the prize is to pay a fee.

The IRS scam, we have heard about that from you, Senator Collins. Someone alleging to be from the IRS calls and scares you into paying thousands of dollars or you will be thrown in jail.

Romance scams. Someone contacts you on a dating Web site and starts "love bombing" you. We can talk about what that means, but it is essentially showering you with praise right out of the gate, even though you do not really know them that well, in an attempt to later borrow money from you.

And the grandparent scam, which we just heard about. This is where, you know—well, I do not need to repeat it. A distressed relative calls, and there is a variety of ways that they do that.

Well, what do all these scams have in common? One thing is the scammer pretends to be someone they are not, and in an age of advanced technology, it has never been easier to do that. One con artist said, "If you are a scammer and you are not using the Internet, you are guilty of malpractice."

The second thing they have in common is that they try to arouse your emotions through fear or excitement in order to get you to make a decision you may later regret. And over the past decade, AARP has interviewed numerous con artists. And when we ask them what their central strategy is for scamming people, they always say the same thing: "Get the victim under the ether." Well, what is ether? Ether is slang for a heightened emotional state that forces the victim to react emotionally rather than think logically.

In 2014, we explored this idea with our partners, AARP, the FINRA Foundation, and the Stanford University Center on Longevity. We wanted to test the role of emotions in making people vulnerable to fraud. We researched whether making a buying decision while in a heightened emotional state makes it more or less likely to fall for a scam. All the con artists said this is true, and

many victims have said this is true, but what does social science say? Can we prove that it is true?

The findings supported this contention that the goal is to get them under the ether and that that, in fact, does make especially older people vulnerable. How did we prove this? Well, in one experiment, subjects played a rigged game in which they initially won money, but then lost continually, leaving them in an angry state. In another experiment, subjects played a game in which they initially lost money and then continually won, resulting in a positive emotional state. And a third group played a game that created no mood change.

Then all three groups were asked to review and rate deceptive advertisements based on their credibility and how likely they would be to purchase. The results were telling: Older people who were in a heightened emotional state, either positive or negative, were more likely than the control group to say they would buy, whether or not they found the ads to be credible. They were also easier to arouse and get into that emotional state than younger persons.

Well, how does this research apply to prevention? For decades now, fraud prevention has focused on this phrase, "If it sounds too good to be true, it probably is." And I have even said that for years. The problem is that only works if you are thinking logically when you are evaluating the scam. And the con man's main goal is to get you out of logic and into emotion. So a lot of our workshops teach this. We teach the persuasion tactics that are done in the service of getting people into a heightened emotional state. When you think of the lottery, you think of a heightened positive emotional state: "I have just won $10 million." With the grandparents it is fear. These are all emotions that are making people vulnerable.

We have dozens of volunteers all over the state, not all of them as productive as Mary here, but many, many volunteers using this research. We have a peer counseling. We have a call center that calls—an outbound call center that calls thousands of people every year and does peer counseling. And this peer counseling is another thing maybe we can talk about later that has been really effective.

I just want to make one final point. Last November, AARP announced a national partnership with the U.S. Postal Inspection Service to warn military veterans about fraud. Eight in ten military victims have received at least one scam attack in the last year, and the number of veterans who report being victimized by fraud is significantly higher than for the general public.

So beginning this week, there will be this brochure, and I have provided these to the Committee. It is called: "They protected us. Now it is our turn." And it really just describes some of the things we have been talking about here today, the common tactics and scams that target seniors, and also allows them to report—and maybe we can talk later about the value of reporting, because I think that is both good for law enforcement to hear from us, but it also has a self-inoculating effect. If you are reporting, if you are looking at these solicitations not because you are interested but because you want to report them, that actually protects you from being scammed.

Thank you very much for your time.

The CHAIRMAN. Thank you for your testimony.
Ms. Bach.

STATEMENT OF MARY BACH, CHAIR, AARP PENNSYLVANIA'S CONSUMER ISSUES TASK FORCE, MURRYSVILLE, PENNSYLVANIA

Ms. BACH. Thank you so much, Senator Collins, for having this hearing today, and thank you, Senator Casey, for your very kind introduction—I also appreciate the attendance of other members of the Committee as well—and for allowing me to share with you my story and AARP's efforts to educate consumers about the frauds and scams that now proliferate almost daily in all of our lives.

My task force team consists of 15 volunteer members from across Pennsylvania who are enthusiastic about educating people of all ages, but especially seniors, about current scams. Our mission statement reads: "The AARP Consumer Issues Task Force will promote consumer protection for all Pennsylvanians, educating members and the public about fraudulent, misleading, unfair, and/or abusive marketplace practices." We educate people about the red flag moments in their lives.

We offer programs and speak before all types of groups, from civic clubs, senior centers, and religious organizations to professional associations, retirement communities, and school groups. I personally share AARP's information with more than 4,000 total attendees in my audiences annually. I couple that with a number of personal appearances on local and statewide television and radio shows, and occasionally even do tele-town hall meetings that reach literally thousands. Pennsylvania Attorney General Josh Shapiro and I did one recently on frauds and scams that had almost 10,000 AARP members tuned in. I have even done a series of videos on YouTube, which were professionally produced by AARP, and they are called "Outsmarting the Scammers with Mary Bach."

There is an old saying, "Each one teach one," and in AARP we are educating many, many people. Education is power. And when someone hears the specifics of a scam, they are much less likely to be victimized. Remember, if you can spot a scam, you can stop a scam.

The Consumer Issues Task Force volunteers offer entertaining and compelling presentations. People need to be engaged in order to better remember the message. We even have a FRAUD Bingo program which we refer to as "Bingo with a message," a fun game, which is educational, also.

Everything we do is centered around fraud prevention. Because of the grassroots nature of our efforts, we have developed strong relationships with many government agencies that appreciate our help in distributing their excellent printed materials to our audiences, such as the Pennsylvania Department of Banking and Securities, our Department of Insurance, our Attorney General's office, and on a national scale, publications from FINRA, the FTC, and the FCC.

While people like to have printed information in hand—and I have supplied all of you with the packets that we distribute to everyone, so I hope you got those—we find that the face-to-face, peer-

to-peer, senior-to-senior interactions generate a trust factor when we are able to swap relevant real-life stories.

After a presentation, I stay and answer questions one on one with people who approach me with a personal story or an unresolved issue related to scams. Many have concerns for themselves or for a loved one who may have been victimized. It is not unusual for some to say, "I wish I had heard your program before I gave money to that contractor, or bought that annuity, or accepted a free medical device I did not need, or actually believed that the guy I met on the Internet was in love with me."

Seniors are being targeted because they are thought to have money available. Older consumers may be less technologically savvy, not understanding how much personal information is available in the public and in cyberspace about them. They are being inundated with phone calls that they cannot control. Scammers are now extensively spoofing their caller IDs to make those they call believe they are calling from a place that fits in with their intended scam, like the local police, the IRS, a charity, or Microsoft. When I say in my presentations that they can no longer rely on their phone's called ID, many in the audience are astonished. Scammers have used my name and number to call intended targets. I learned of it when I received a call from someone I did not know that I had not called asking why I had phoned her. She said that she was returning my call to the number that showed up on her caller ID.

Imposter scams are the worst. Like many others, I have received calls from the tech support scam, the federal grant scam, charity scams, sweepstakes and lottery scams, and others. A man in Syria sent me a Facebook message telling me he wanted to marry me. I assure you, my husband might have objected.

[Laughter.]

Ms. BACH. My husband has answered the phone to hear the jury duty scam, the grandparent scam, among others. And the bottom line is that all of these scams are about money, the potential victim's money, and that is why education and vigilance are imperative. When people understand, they will hang up the phone. And I always give my audience members permission to be rude.

AARP does not want anyone to fall for a telephone line, and in that regard, AARP has initiated a national program called the "Fraud Watch Network." Consumers of all ages can sign up to receive fraud alerts about current scams that are going on in their communities. It is free of charge; no membership is required. And I am proud that Pennsylvania leads all the other states in Fraud Watch Network sign-ups. And I hope each and every one of you will sign up with me today, and I have given you all sign-up sheets.

AARP sponsored a Hackathon contest here in Washington, challenging student teams from prestigious universities to come up with innovative ideas to help prevent or stop scams. The suggestions proposed by these students would help stop robocalling scams and caller ID spoofing. The technology that has made the ability to scam us easier for crooks can certainly be adapted to work for consumers and not against them.

I thank you all for the opportunity to be here today as someone who is in the trenches day to day trying to make a difference in helping to diminish or eliminate the number of people being victim-

ized by scams or frauds, and you know I would welcome your questions.

The CHAIRMAN. Thank you very much, Ms. Bach, for your great work.

Ms. BACH. Thank you.

The CHAIRMAN. Ms. Omansky.

STATEMENT OF ADRIENNE OMANSKY, FOUNDER, STOP SENIOR SCAMS ACTING PROGRAM, LOS ANGELES, CALIFORNIA

Ms. OMANSKY. Good afternoon, Senator, fellow testifiers, and guests. Thank you, Senator Collins and Senator Casey, for inviting me to this important hearing. It is an honor to be here to provide testimony on how my program has had an impact on stopping senior scams.

Our program began in 2009, and we are a total volunteer group. In the last few years, we have grown and have performed in about 30 venues per year, from a small veterans group to the convention center with over 1,000 seniors. We have 26 skits in our repertoire, with 27 actors ages 65 to 99. We always include the Medicare, IRS, and the I Won a Prize skits. In every venue, the seniors have experienced many of the same scams, including the IRS and grandparent scams. One of our own cast members, Janey, was a victim of an insidious form of the grandparents scam. The scammer got information from her Facebook page and threatened to kill her granddaughter if she did not send the money being demanded. Janey sent the money. She now feels empowered by telling her story to other seniors.

Our program is always evolving, changing, adding, and creating. We have help in crafting our skits from a professional theater and performance arts center. Although we use many aspects of theater in our skits, including puppets, this is not enough to educate our audience. We collaborate with professional organizations to make sure our information is accurate, such as Senior Medicare Patrol and the Federal Trade Commission.

After each skit, our former judge, Francine Lyles, or one of our educators explains the scam to the audience. The finale of the program includes all cast members singing the "Just Hang Up" song, and each actor steps forward and tells the audience if they were a victim or a target of a scam. At the conclusion of the program, the audience is asked to fill out a comment card to tell us what they liked or may suggest. Bookmarks from Senior Medicare Patrol and the Federal Trade Commission are always given out. In addition, materials are available from the city and county district attorneys' office in several languages.

Our audience members often tell us what they have learned from our programs, but what have we learned from them?

We have learned that scams are under-reported because seniors sometimes do not know where to report them to. They are ashamed of reporting them, and sometimes think it will not help.

We learned that they are embarrassed to tell their family members, including their spouses. They sometimes are afraid to tell law enforcement.

We learned that they are more likely to tell their peers than anyone else.

We learned that sometimes seniors do not like professional fraud prevention programs because they often feel condescended.

We learned that seniors who live in assisted living facilities are particularly vulnerable to scams because they are lonely and they want to win money to help their children and grandchildren.

We have learned that seniors who have been scammed have emotional scars.

We have learned that anyone can be a victim, regardless of education, race, gender, national origin, or social economic background.

We have learned that seniors are the ones to stop senior scams.

We have learned that theater is a wonderful platform to educate.

We have learned that peer-to-peer education works.

The peer-to-peer model provides a comfortable and safe environment where they can identify with people who have similar life experiences, both as targets and as victims of scams.

The people who disseminate the information are non-judgmental. This gives the seniors in the audience the opportunity to open up and honestly share their own experiences.

The thread throughout our peer-to-peer presentation is empowerment in that only you and I can stop these senior scams. We are all in this together.

And now I would like to present a short video on our program.

[Video played.]

The CHAIRMAN. Thank you very much for that very powerful testimony, and you certainly hit home the message with that video. Thank you so much.

I am going to start with Mr. and Mrs. Shiman in my questions, and first I want to tell you that probably 8 to 10 years ago, on a very busy day here at work, all of a sudden an e-mail popped up, and it appeared to be from my nephew. And he said that he was overseas, that he had been mugged, that his passport, his airline ticket, and his wallet had been taken, and that he and his friend were OK, but they were very shaken up and they had absolutely no money and no way to get back home, and could I please wire him some money.

Well, fortunately, I was not under the ether, or perhaps I am just a little more hard-hearted than the Shimans, but I told him to go immediately to the American embassy and did not wire any money. I then started thinking about it and called his father and found that he was exactly where he was supposed to be in the United States. He was not overseas, much less mugged.

But I tell you this story because although I never wired the money, for a very brief time I was convinced it was my nephew. It sounded like him. It had his e-mail address. He was in his 20's at the time and traveled a lot, and it was totally feasible. And so I shared that story because I think it shows that these thieves are very clever and they are ruthless.

So I want to ask you a question. You mentioned in your testimony that you drove to Western Union and sent your money, more than $1,200, to the Dominican Republic. Did anyone at Western Union question why you wanted to send that large sum of money to the Dominican Republic?

Mrs. SHIMAN. Well, this is very interesting because in Maine, I think in a lot of towns—and I learned that that is the same thing

in Massachusetts—the Western Union office is often in a supermarket or a drugstore, a pharmacy, some other business. They do not have separate offices.

One of the interesting things is that this Mr. Diaz, the public defender, said to us, "By the way, I know where there is a Western Union office in Saco," he said. "It is at the Hannaford on Main Street, and they have a booth there."

So we withdrew the money from the bank and went to Hannaford, and at the service desk, there were two or three people—there was a sign there that said "Western Union." There were two or three people there servicing customers, and one fellow said to us, you know—we said we have to send money through Western Union, and, you know, while he is bagging milk and eggs and bread, he is handing us the forms, and he just took them and that was he end of it. No one said a word to us. No one.

And even in the bank—and this is another thing that we have discussed, that the banks, too, I think share a little bit in this. When they see someone come in and say suddenly, you know, "I am withdrawing $1,250 in cash," that should also raise something in their minds. And we discussed that in the office this morning. But, no, no one at Western Union suggested anything.

The CHAIRMAN. You will be pleased to know that Western Union is entering into a settlement because of those kinds of activities, and also that the banking bill that is on the Senate floor includes legislation that many of us have co-sponsored called the "Senior$afe Act," and it is modeled on Maine's law so that if a bank employee or credit union employee sees something suspicious, they will not hesitate to question it and can do so without being concerned that they are going to be sued. And I think we have a very good chance of finally getting that through, because I know a lot of alert bank and credit union employees in Maine who have asked that question due to the protections in Maine law and stopped a fraudulent transaction from going through.

Mr. SHIMAN. And I just want to add to what Rita said, that if someone had said, "This does not look right," the chances are in this situation we would not have done it. So it is very important.

The CHAIRMAN. You anticipated my next question, so thank you for adding that.

Mr. Shadel, I know you have done a lot of research in this area, and we know that veterans are disproportionately affected, as you mentioned in your statistics. Do you have research that shows that particular kinds of scams are directed at particular population groups? Are there certain demographics that link up to specific scams?

Mr. SHADEL. You mean for veterans or just in general?

The CHAIRMAN. In general.

Mr. SHADEL. In general, yes, we have done—thank you for that question. We have done a lot of profiling research over the years. You know, we used to in the fraud prevention world figuratively fly over a football stadium and drop 60,000 brochures out onto that stadium hoping that by reaching everyone we would also reach the smaller subset that are victimized. That is not a very efficient way to do fraud prevention, which gave rise to this whole body of research about profiling.

So we, for example, created—you know, surveyed known victims of lottery fraud and the general public to see how they differ from the general public, same with investments, same with veterans now. So we have got some pretty well developed profiles, and a lot of times they are very different.

For example, take investment victims and lottery victims. At first we lumped them together and compared them to the general public, and there was no difference. That is because when you separate them out, they are precisely divergent. The lottery victim tends to be female, tends to be over the age of 70, lower educational attainment, lower income. Investment fraud victims are more likely to be men, 55 to 62, higher education, and you are going to reach those people in completely different ways with completely different messages. Likewise at veterans. This brochure is informed by profiling research we did with veterans, with U.S. Postal Inspection Service.

So we are getting a little smarter about it. You can customize the message that way, and you can target it and hopefully it is more efficient.

The CHAIRMAN. Thank you.

Senator Casey?

Senator CASEY. Thanks very much.

I will start with Mary. I have been referring to you as "Mary." I hope that is OK.

Ms. BACH. Please do.

Senator CASEY. Mary, by the way, you talked about YouTube. I hope we can get your testimony on YouTube. That would, I think, scare the hell out of these scammers.

Ms. BACH. I would hope so.

[Laughter.]

Senator CASEY. And I mean that as a compliment, in a very good way.

These scams continue to proliferate across the board because these bad actors find very creative ways to take hard-earned dollars from folks. One of the audiences we are trying to reach here are employers, whether they are banks or retailers or pharmacists or wire transfer companies. We know that banks that see a large sum of money coming out of an account in a sense get a heads up or have an indication of something. Retailers sell gift cards that many victims use to pay the con artists. Some of these employers have stepped up to protect customers, but more companies need to take action.

Just the basic question is: What more can employers do, what can we do to encourage employers to focus more on this and also to take steps to prevent these scams?

Ms. BACH. Well, as I said in my testimony, I am just such a firm believer in education, I really do think education in any way is the key to alerting everybody about these kinds of scams. And to piggyback on something that the Shimans said about people being educated or the bank tellers knowing, I think we all have to remember that it is the consumer's money and they can do whatever they want to do with their money, even if it is giving it to a scammer. And sometimes even when a retailer or a bank teller is well educated and may actually try to intervene in some of these situations,

the person is in the ether so much or so headstrong about it that they do not care what they are told, and they literally go headstrong in it and send their money and allow themselves to be scammed.

But any way that retailers or bank tellers, any employer can get the information, possibly through video training behind the scenes, as part of just the employment process, there are ways to train employees about what they might expect from a customer who, again, has a large amount of money. And if something seems out of kilter a bit, if you have got the little 80-year-old grandmother coming in and wanting to buy $1,500 worth of iTunes cards, I think that is a bit of a red flag in somebody's mind. And if that employee, without fear of any retribution, without fear of a lawsuit possibly after the fact, could ask questions or say, "How are you using that money?" or, "May I ask, do you have a lot of grandchildren that you are buying iTunes cards for?" or "What is this for?" possibly the person, again, would open up. As the Shimans said, if somebody had said something to them or questioned them in the process, they might have been willing to take a double look.

So anything an employer can do to train employees, even having a little card at the checkout, a sign up saying, "Is it possible you are being scammed if you are taking a lot money out of your bank account?" whatever it is. Any step is a small step in the right direction.

Senator CASEY. And the other question I had, Mary, was an idea that has been suggested is to have a federal task force to develop standard educational materials. What do you think of that kind of approach in terms of a federal initiative?

Ms. BACH. I think that standardization of materials is certainly a good start. Education is key, and I mentioned having printed materials in hand for all of our audiences. People want to go home and digest some of this in the privacy of their home after they have heard a certain pitch through a presentation. And when they can step back and read and know that there are agencies out there that are willing to help them—at AARP in Pennsylvania we have what we call the "Consumer Issues Reference Sheet," and we literally give out toll-free telephone numbers about agencies that are there to help all of us in terms of knowing about frauds and scams, or if someone has been scammed, how to go about reporting it, et cetera.

And so I think any task force that can further the cause, that can really look into some of the technological situations that are occurring, this ID spoofing, this robocalling, we will be a step in the right direction and maybe a step ahead.

Senator CASEY. Thanks very much.

The CHAIRMAN. Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you. Thank you, Madam Chair and Ranking Member. And thank you to all of you. Thank you for coming forward today. This is such an important topic because it impacts all of us and all of our communities.

I just want to say to the Shimans thank you for coming forward. Your voice matters, and you talking about it today is going to prevent somebody else from becoming a victim. And to everyone else here, your work and effort is key.

Let me start with this question, because I have worked on this issue in Nevada, particularly to protect seniors against these types of fraudulent activities and scamming. And I agree with you, I think education awareness is the first step in that prevention. Education is key. Education, education.

The first time I have heard peer-to-peer being so effective, and I like that idea. So what I am going throw out there is ask you, Mr. Shadel and Ms. Bach and Ms. Omansky, what was the most effective? What is the most effective outreach that you have found to really connect to seniors to educate them on the scams?

Ms. BACH. Well, I said in my testimony that I think you have to engage them. It has to be compelling. We do it with humor. We tell individual stories about things that have actually happened to us. We talk about scamming the scammers. I will tell you that I do not mind jerking them around on the phone a bit, and, again, I give my individual audiences permission to be rude. And I had the federal grant call, and some of you may not be familiar or heard about the federal grant. But with a lot of talk in the news about the economy improving somewhat and some of the initiatives that the government is wanting to take to improve the economy, I got a call from a guy who had a very-—an accent that was very difficult to understand, and he told me I had won the federal grant and that it was $9,300, and I got very excited on the phone. And I asked him what it was for, and he said, "We want you to go out and spend it and stimulate the economy." And I said, "How do you want me to use it?" He said, "You can pay bills. You can go shopping." Music to my ears.

And so then he said, "But I have to have some information about you." He verified my name, which is available in the phone book or on the Internet, and my street address. And I live in Murrysville, Pennsylvania, but he had me in Raleigh, North Carolina. So, of course, I verified for him that I did live in Raleigh, North Carolina, with that Zip code. And then he said, "And we have to know your age." And I said, "A gentleman should never ask a lady her age." And then he started guessing, and he said, "If I guess, will you tell me if I am getting it right?" And I said, "Give it a try." And he started at 75. And I said, "That is much too old." And then he started going down in 5-year increments. I evidently think he only thought he could go down. And every time he took 5 years off, I told him he was not correct. And so he kept guessing.

When he got to 60, I said, "Oh, it sounds good." And so he had me in Raleigh, North Carolina, at 60, and then he told me to go to a Moneygram store. And I was actually talking on my landline in my kitchen to this guy, who I am sure was out of the country, and I have never actually bought a Moneygram, but I know what they are. And so he said, "Go to the Moneygram store in your community and wait for our call." Well, if I had gone to the Moneygram store, I would still be standing there because he would be calling my phone in the kitchen. So that was the end of that conversation.

A week later, I got a similar call from a different voice on the phone telling me I had won the federal grant. And so I played along again, and this time he said it was for $4,000. And I said, "Oh, my goodness. Last week the guy promised me $9,300."

[Laughter.]

Ms. BACH. And he hung up the phone on me.

So those are the kinds of stories we tell, and we talk about what we do in a fairly entertaining fashion, and people like humor, and sometimes people remember more when they hear a funny story or they see somebody waving a red flag, and giving them permission to hang up the phone and not have to talk politely or with trust to the person who has called them and interrupted their dinner hour.

Senator CORTEZ MASTO. Thank you. And I notice my time is up. I just have a quick question. So how do you connect, where do you go to connect to your peers? And I guess for the Shimans, if you were to get this education, where would you have gone? I mean, unless you are aware of the education that is out there, that AARP is doing it or the forms are there, how do we make sure people know. How do we make sure seniors know where to go and connect the two of you?

Mr. SHIMAN. Speaking for us, we live Saco, Maine, and we have had this happen in the community as a growing thing in Maine. We call it "Age-Friendly Communities" that circulates information about things like this. That is the way—I am active with that organization, and that reaches out to seniors in big numbers.

Senator CORTEZ MASTO. Good.

Mr. SHIMAN. So I think that you look for that kind of organization, AARP or other agencies.

Senator CORTEZ MASTO. And connect.

Mr. SHADEL. Can I just add one thing? We do have—there are fraud fighter call centers. We have one in Seattle and one in Denver. The number is in this brochure. And those are volunteers. Those are peers answering the phones, and they will talk to the person as long as they need to, to get them where they need to go. So people can call us.

Senator CORTEZ MASTO. Thank you.

Ms. OMANSKY. I would like to add something. My group have all been victims of scams, and, of course, everyone has been a victim of a target. So the most effective way that my group educates the seniors that we go to is to come into the audience after our program and talk to them on an individual basis. And this is different because it is like a support group right there. We do not leave after our program. We are there to answer questions. And we have veterans in our program. We have four, and they are in the field talking to veterans, and they bring back to us what the concerns are of the veterans and what the scams are. And we find out some scams that no one has ever heard of.

There is a reverse grandparent scam, and we encourage our seniors, especially when we are in libraries and it is open to the community, to bring their grandchildren and their children. And we found out that young people are now getting calls that their grandparents are in jail—not in jail but have gotten into an accident and they need money. And we have prevented two of these scams, and we found this out twice that this is happening in Los Angeles.

So we are sure there is more out there. So that bond that we talked about is very, very special, and that bond, grandparents can talk to grandchildren, sometimes they cannot talk to their children.

Senator CORTEZ MASTO. Right. Thank you. And I know I have gone over my time. Thank you.

The CHAIRMAN. That is fine.

Mrs. Shiman, you look like you wanted to add something.

Mrs. SHIMAN. Yes. To me, the most powerful thing is one on one. You tell your friends, and this is what we found out. The point is that when people are scammed, they do not want to talk about it. And once you let it out, the pipeline starts flowing, and somebody will tell somebody else, "Did you know the Shimans were scammed?" And I think you have to make it very personal in addition to all of these other things. You have to feel that it can happen to you. If it happened to them, it can happen to you.

Ms. BACH. And, Senator, from the perspective of the presenter or the person who is providing the program, you have to know your audience. You always have to know the types of people that are in your audience, and that is why we find FRAUD Bingo to be so very successful in Pennsylvania, because we play Bingo with a message, and we call the numbers, but it is F–10 or D–60 as opposed to B-I-N-G-O. We use the word "fraud." We provide the prizes, and with every number that we call, we give a tidbit about fraud, like, "Investigate before you invest," or "Do not trust caller ID," a simple message that resonates with people in the audience and they can have fun and learn at the same time and maybe win a prize.

The CHAIRMAN. Thank you.

Senator Blumenthal?

Senator BLUMENTHAL. Thank you all for being here. I have another hearing I am going to have to rush to now. But let me just say I sort of feel like there is an elephant in this room, which is where are our law enforcers, right? The Western Union settlement I thought had been concluded years ago. Why are we permitting established institutions to aid and abet these kinds of schemes? They have the ability, in fact, they have increased ability with modern technology to stop them. And if it were a priority, if our law enforcers at both the state and federal level took a more aggressive role here, and if we passed a statute I happen to have proposed—I have no pride of authorship—the Robert Matava Elder Abuse Prevention and Prosecution Act that would require mandatory forfeiture when these people are caught so that there are real penalties and also prison terms for this kind of fraud, I think we could really assist our seniors. I think word of mouth is great. I think education is fine. But at the end of the day, what these people understand is the criminal justice system, and that in turn also would publicize more of these schemes.

So I want to thank you all for being here, and I look forward to working with you.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator. Before you came in, I mentioned that the Justice Department has just announced a new initiative in this area, and the appointment in every one of the 94 U.S. Attorney's Offices of an elder fraud prosecutor, essentially. So I think you are absolutely right, there has been a lack of information—or focus by law enforcement on this, but I am hopeful that we are on the right track now. And, of course, for state officials,

if the call center is in India, it is very difficult for state officials to do anything about it.

I just want to ask one final question and give each of my colleagues a chance in case they have one as well.

Ms. Omansky, in 2015, Congress mandated that Medicare remove the Social Security number from Medicare cards by the year 2019 because people could see that number and it was being used for fraudulent purposes. So Medicare is now mailing out new cards to all enrollees beginning next month, and many of us have really pushed for this. And the cards are free, but guess what? Not surprisingly, scammers are using this new policy to try to trick seniors into paying for their new cards.

Could you please talk about what you are doing with the Senior Medicare Patrol to warn seniors that they should not pay for these cards, that they are free?

Ms. OMANSKY. Thank you very much for asking that question, Senator. We collaborate with Senior Medicare Patrol, and they have a new bookmark out which explains what the card is going to look like, and it explains the fraud. We take this card to every one of our performances, and we have it in ten different languages.

Also, we just collaborated with them on a video in which an older woman and her son discuss a potential scam about the Medicare card. Now we take that into our performances, and we act it out live with the same actors, because the two actors in the video are a part of our program, and this is very successful because we show it three ways: we show it written, we show it in a video, and we show it live.

The CHAIRMAN. That is great. Thank you.

Senator Casey?

Senator CASEY. I just have one question for Mr. Shadel. Based upon some of the testimony we heard today from Mary talking about her travels, the many miles, I think our staff did a rough calculation, Mary, and I guess if you are at 15,000 miles, it means you have driven across the state 53 times. I just hope you do not run for office.

[Laughter.]

Senator CASEY. But no matter how many miles she travels or how many times she would go across the state, of course, she cannot prevent every one of these. So we have got to get at the root causes. We know the FTC finalized the new rule that I mentioned to allow the phone companies to block calls. But obviously this problem of spoofing fraud is still happening.

I guess the basic question I have is: What can we do to ensure that the industry is using this new tool and every other possible tool to prevent this? What is your sense of that?

Mr. SHADEL. Yes, we definitely supported that move of the FTC to allow telecommunications companies to use the technology that we know exists to slow down these robo-dials. When we survey our members, one of the—this neighbor spoofing thing is what really kind of, excuse the expression, freaks out our members because it is like they have got the area code and the prefix, that is my area code and prefix. I get these myself. And there has been an astronomical rise in not just robo-dials but that particular kind of robo-dial because people pick it up. We are starting to wise up to it. And

so anything we can do in the way of enforcement, holding the feet to the fire of the telecommunications companies to use the technology that we know exists—I mean, in 2013, the FTC had a design challenge—you may recall this—where I think Nomorobo was the winner, and this was simply a blacklist data base that he created by buying old phone lines and then monitoring them and identifying—this particular company identifies 1,000 new robocallers a day. So we know that the technology exists to be able to identify those and block them. We just need to get them to do it.

I am always astounded whenever I see the new FTC Consumer Sentinel report coming out that still, in terms of complaints coming into Consumer Sentinel, 70 percent of the way these consumer fraud people are contacted is by phone still. Even with all the e-mail technology and the texting going on that we hear about, a lot of it is still the phone. And one of the things—and Mary and I have talked about this—that we give people just as a tip is we teach them to use a refusal script. A lot of our folks, when you survey our members, say, "I do not want to be rude," "I do not want to hang up the phone." So we say, "OK, you do not have to be rude, but write a sentence or two down. I will help you. How about this? 'I am sorry. This is not a good time. Thank you for calling.' Put that phrase by the phone so you can disconnect." Because if you get on the line with them, it is like playing one-on-one basketball with an NBA player. You are not going to win.

So, anyway, you know, the robo-dial thing is—nothing riles up our members more than just picking up the phone and they do not know who it is, or they hear nothing and they do not know who that is, and they get worried about it.

Senator CASEY. Thank you.

The CHAIRMAN. Senator Casey, I am so glad you brought up that last issue and that Mr. Shadel had the opportunity to respond, because years ago, when the Do Not Call Registry was established, we had hoped that we were going to see an end to these kinds of abusive calls. And the ability to spoof the telephone number has really made the Do Not Call Registry useless. And I share your frustration that the telecommunications companies have technology available that could help in solving this problem.

Mr. SHADEL. Absolutely.

The CHAIRMAN. And they need to deploy it. And it would make such a difference.

I am personally not surprised that the telephone is still the instrument of choice by con artists because it is harder to have an emotional connection through e-mail. Romance online scams do exist, but it is when you hear someone on the phone and you do not want to be rude, and you may be isolated and living alone, that it can become very seductive to be drawn into a scam. And I think your refusal script is a really good idea and one that we should add to next year's Fraud Book as one of our tips for people.

As our Fraud Book and the extensive hearings that we have held make clear, criminals are absolutely ruthless in their pursuit to swindle seniors out of their hard-earned savings, and we have heard truly tragic stories of people losing their life savings. And we need to crack down on this from several perspectives. I am pleased that we are finally seeing a concerted effort by the Department of

Justice, which is long overdue. The FTC in my judgment could do more as well. The telecoms could do more.

But I want to thank you for your efforts because the best thing we can do is to prevent people from becoming victims in the first place. If these con artists have to make 1,000 calls before they get one victim, that not only is going to slow them down, which is why I love that Ms. Bach keeps them on the phone so long.

[Laughter.]

The CHAIRMAN. It is not only going to slow them down, but they are going to move on to something else, a more cost-effective way of trying to commit a crime. We will have to go after that, too. But educating people about these crimes is absolutely imperative, and we know we have a wave of baby boomers who are going to be the new silver tsunami, and there are some who actually call financial fraud the crime of the 21st century and that it is just going to keep snowballing if we do not keep being relentless in our fight back against fraud.

So I am very encouraged about the efforts that you are undertaking, and to the Shimans again, a special thank you to you for putting a human face on those who have been victimized, and your coming forward will help prevent others from becoming victims as well, which we very much appreciate.

Mrs. SHIMAN. Thank you very much.

The CHAIRMAN. Thank you.

I look forward to continuing to work with Senator Casey, my Ranking Member, and the other members of this Committee in order to fight for and protect our Nation's seniors.

Senator Casey, any final thoughts?

Senator CASEY. Thank you, Madam Chair, and I share that sentiment. I think everyone is determined to keep working together on this. The bad guys are creative. We can be as creative and as determined as they are. And this is one of the days we have more information because of your testimony and because of your lived experience in dealing with this.

I have to say, Mrs. Shiman, when I was listening to the first part of your testimony, you had me, even without any kind of emotion. I probably would have fallen for that. I hope I would not have, but just the recitation of it was very compelling.

So we have a long way to go, but I think today is one of those days we can really shine a light on this, and we are particularly grateful for the Chairman and her work on this for many years. And, Mary, I hope everybody in Westmoreland County who is thinking about taking you on is on guard, because you are ready to meet them.

Ms. BACH. Thank you, Senator.

Senator CASEY. Thanks very much.

The CHAIRMAN. My thanks to all our witnesses, and also to our staff, which has worked very hard on this issue and cares deeply about it as well.

Committee members will have until Friday, March 16th, to submit any questions for the record, and if we get some, we will be passing them your way.

Thank you again, and this concludes our hearing.

[Whereupon, at 2:23 p.m., the Committee was adjourned.]

APPENDIX

Prepared Witness Statements

Prepared Statement of Rita and Stephen Shiman, Grandparent Scam Victims, Saco, Maine

Good morning. Thank you for your interest in the problem of scamming of senior citizens. We also want to thank our friend, Sheriff Bill King of York County, Maine, for his work in educating seniors about scamming.

Indeed, there is a special bond between grandparents and their grandchildren. The scammers knew this well and took full advantage of it with us. They knew that when a grandchild is in trouble, grandparents go all out to help. There also was a concern on our part of potential racial bias in this situation.

On the morning of May 28, 2015, Rita answered the phone and spoke to someone who said he was our grandson, Kabo, who is an adopted native of Botswana. She said it sounded just like him. He said he was in Atlanta, Georgia and that he had been arrested and was in a county jail. He needed bail money. She asked him what brought him to Georgia from his home in Maryland. He said a college classmate had died of cancer and several friends drove to Georgia for the funeral.

Kabo told Rita he was assigned a public defender who promised him he would be freed upon payment of bond satisfactory to a judge. He was turning to us, because he didn't want his parents (our son and his wife) to know. He made Rita promise she would not tell anyone about this. He said the public defender would call us shortly.

The supposed public defender, identified as George Diaz, did call us and said he was meeting with the judge shortly. There was a sense of urgency. If we paid $1,230 the judge would release Kabo. He said the transaction had to be in cash and sent via Western Union to his contact in the Dominican Republic, and he gave us the details. That statement alone should have raised a red flag, but we were so caught up in the moment that we were simply acting on autopilot. He also said that if Western Union questioned this transaction, we should say nothing. He said they legally have no right to ask. As it turned out, no one raised an eyebrow.

When we returned home after making the payment and calmed down, we began to have second thoughts, especially after we received another call from the public defender that he had met with the judge and the amount we had sent was not enough. Stephen called the public defender's office in Atlanta and learned there was no one by the name of George Diaz. Stephen then called our son's house. Kabo picked up the call. He never was in Georgia!

It's very easy to play Monday morning quarterback. There were so many red flags. We replayed the entire incident over and over, and couldn't believe we had been so duped. Hopefully, through the work of this committee and that of AARP we can find a way to prevent others from becoming victims of this malicious activity.

Prepared Statement of Doug Shadel, Ph.D., State Director, AARP Washington

Thank you Chairman Collins, Ranking Member Casey and Committee Members for the opportunity to talk about the current state of consumer fraud that targets older persons in the United States. I would like to briefly mention three things in my remarks today:

(1) Provide an overview of the most common scams we see going on in the marketplace;
(2) Describe some of the newer research we have done with colleagues at Stanford University, the FINRA Foundation and the U.S. Postal Inspection Service about what makes consumers particularly vulnerable to scams and fraud; and
(3) Describe how we have applied some of this research to our outreach and prevention programming in the field.

Common Scams

The biggest single area of fraud we see is the rise of imposter scams. The FTC's Consumer Sentinel reports that the number of fraud complaints involving imposter scams has risen from about 120,000 in 2013 to over 400,000 in 2016. AARP did a survey last year and found that the top imposter scams were:

(1) Tech support scams—A pop up appears on your computer telling you that you have a virus and to call a toll-free number to have it removed. The scammer charges an arm and a leg to remove what is often a non-existent problem.
(2) Phishing scams—P-H-I-S-H-I-N-G—These are notices you get via mail, e-mail or text that look like your bank or your credit card company and they tell you to contact them with personal information to fix a problem with your account. The scammer's goal: steal your personal identifying information.

(3) Lottery scams—Someone calls or writes and tells you that you may have won the Jamaican or Spanish lottery and all you need to do to claim it is pay a small tax or fee.
(4) IRS scams—You get a call that tells you that you owe the IRS thousands of dollars and you need to take care of it immediately or you will be arrested and thrown in jail.
(5) Romance scams—Someone contacts you on a dating Web site and starts "love bombing" you—showering you with praise and declaring their love within hours of first meeting in order to convince you to send them money.
(6) Grandparent scams—This is the scam we just heard about, where someone calls posing as a distressed relative who needs money to get bailed out of jail.

Now you might ask yourself what do these scams have in common? One thing is the scammer is pretending to be someone they are not and in an age of advanced technology, there has never been an easier time to do that. One scammer told us if you are committing fraud and you are not using the internet, you are guilty of malpractice.

The second thing they have in common is they are trying to arouse your emotions through fear and/or excitement in order to get you to make a decision you may later regret. This leads me to discuss some of the research AARP has conducted about the role of heightened emotions and fraud victimization.

Over the past decade or so, we have interviewed numerous con artists about their crimes. When we ask them, "What is your central strategy for defrauding consumers?", they always say the same thing: get the victim "under the ether." What is ether? Ether is slang for a heightened emotional state that forces the victim to react emotionally rather than think logically. The idea is that when someone is in an emotional state, whether it is being joyful because you may have just won the lottery, or fearful because your grandson is in a Canadian jail or you have just been told you owe the IRS thousands of dollars, the logical reasoning part of your brain is swamped out by the strong emotions of the moment and the victim is more likely to make what academics call "a suboptimal decision" that leads to being scammed.

In 2014, AARP and the FINRA Foundation teamed up with researchers at Stanford University to test the role of emotions in fraud. The research question was this: does making a buying decision while in a heightened emotional state make it more or less likely one will fall for a scam? We tested this by bringing older and younger people into a lab in Palo Alto. In one experimental condition, subjects played a rigged game in which they initially won money but then lost continually. This left them in an angry emotional state. In another condition, subjects played a rigged game in which they initially lost money, then had a continual winning streak, which put them in a mood of positive excitement. A third group played a game that created no mood change.

All three groups were then asked to review and rate deceptive advertisements based on their credibility and how likely they would be to purchase the item. The results were telling: Older people who were in a heightened emotional state (positive or negative) were more likely than the control group to say they'd buy, whether or not they found the ads credible. They were also easier to arouse emotionally than younger persons or controls.

This finding supports the con artist's contention that getting consumers "under the ether", especially older people, creates a vulnerable moment in which they are more easily manipulated and therefore more easily scammed.

How does this research apply to prevention? Well, for decades now, the clarion call of fraud prevention practitioners everywhere—and I admit—I have used this myself—has been "If it sounds too good to be true, it probably is." While this statement makes perfect sense, it is only effective if you are thinking logically. But the con man's first and really only goal is to get you away from logic and into emotion and keep you there as long as possible. As a result, relying on this "too good to be true" phrase is like locking your money in a safe where the thief has the combination.

Much of what we do in our workshops in local communities is to teach consumers the persuasion tactics scammers use to get the victim under the ether. We teach them about the phantom wealth tactic, which is dangling the prospect of winning the lottery as a way to get you excited. We teach them to spot fear tactics like the grandparent scam where they claim your grandson or daughter is at grave risk.

We also use this research in our AARP Fraud Fighter Call Centers in Seattle and Denver that make outbound and inbound calls to consumers all over the country. Dozens of volunteers provide peer counseling that reminds folks how the scammers operate and the sneaky emotional manipulation they use to trick you. These peer counseling interactions have also been tested by Stanford social scientists and those who received such calls are significantly less likely to get scammed as a result. I

have provided committee staff with copies of these studies should you want to read more.

Because so many of the scams seniors fall for are still done over the phone, we provide older consumers with what we call a "refusal script" that allows them to more easily end an interaction with a potential scammer. AARP focus group research found many older consumers find it difficult to discontinue a conversation with a scammer or an unknown caller because they don't want to be rude. We advise seniors to write out a script and put it by the phone so that if they need to end the call, they have something to say without being rude. What's an example? "I'm sorry, this is not a good time. Thank you for calling."

One final point: last November, AARP announced a national partnership with the U.S. Postal Inspection Service (USPIS) to warn military veterans about fraud. Research shows that 8 in 10 military victims have received at least one scam attack in the last year and the number of veterans who report being victimized by fraud is significantly higher than for the general public.

Beginning this week, Americans who visit more than 30,000 post offices around the country will find written fraud prevention materials that can help military veterans avoid scams that specifically target them, including VA loan scams, pension poaching and aid and attendance scams.

Thank you for the opportunity to participate in this hearing this afternoon.

Prepared Statement of Mary Bach, Chair, AARP Pennsylvania's Consumer Issues Task Force, Murrysville, Pennsylvania

Good Morning. My name is Mary Bach and I am from Murrysville, Pennsylvania, a suburb of Pittsburgh. Thank you Senator Collins, Senator Casey, and Members of the Committee for allowing me to share with you my story, and of AARP's efforts to educate consumers about the frauds and scams that now proliferate almost daily in all our lives.

I am a former high school teacher and a long-time consumer advocate with a history of activism on a wide variety of consumer rights issues. I was honored in 1999 at the National Press Club in Washington, DC as "Consumer of the Year", and in 2002, was invited to join Governor Schweiker as he signed into law the Commonwealth's "Do Not Call" legislation, for my assistance in helping the public to understand its significance. In 2004 I was the recipient of the Andrus Award for Community Service in Pennsylvania, the highest volunteer award given within AARP.

I have been a lead volunteer with Pennsylvania AARP for almost 20 years, chairing their Consumer Issues Task Force. As you are probably aware, AARP is the largest organization for people over 50 in the world, advocating for seniors on a wide variety of critical issues. My task force team consists of 15 volunteer members from across Pennsylvania who are enthusiastic about educating people of all ages, but especially seniors, about current scams. Our Mission Statement reads: "The AARP Consumer Issues Task Force will promote consumer protection for all Pennsylvanians, educating members and the public about fraudulent, misleading, unfair, and/or abusive marketplace practices". We educate people about the red flag moments in their lives.

We offer programs and speak before all types of groups, from civic clubs, senior centers, and religious organizations to professional associations, retirement communities, and school groups. I personally average approximately 15,000 driving miles per year across Pennsylvania, presenting at 100 or more events and sharing AARP's information with more than 4,000 total attendees in my audiences. I couple that with a number of personal appearances on local and statewide television and radio shows, and occasionally even do tele-town hall conferences that reach thousands. Pennsylvania Attorney General Josh Shapiro and I did one recently on frauds and scams that had almost 10,000 AARP members tuned in. I've even done a series of videos on You Tube, which were professionally produced by AARP, called "Outsmarting the Scammers with Mary Bach".

There's an old saying. "Each one teach one" and in AARP we are teaching or educating many, many people. We know that education is power and, when someone hears the specifics of a scam, they are much less likely to be victimized. If you can spot a scam, you can stop a scam!

The Consumer Issues Task Force volunteers offer entertaining and compelling presentations, knowing that people need to be engaged in order to better remember the message. We even have a FRAUD Bingo program which we refer to as Bingo with a message, a fun game, which is educational, too. Everything we do is centered around scam prevention.

Because of the grass roots nature of our work and mission, we have developed strong relationships with many government agencies that appreciate our help in distributing their excellent printed materials to our audiences. This would include the Pennsylvania Department of Banking and Securities, our Department of Insurance, the Commonwealth's Attorney General's office, and on a national scale, FINRA, the FTC and the FCC. While people like to have printed information in hand, the face to face, peer to peer, senior to senior interactions generate a trust factor when we are able to swap relevant real life stories.

After a presentation, I often will stay and answer questions one on one with people who approach me with either a personal story or an unresolved issue related to what we outlined for them. Many are animated by concerns for themselves or a loved one who may have been victimized by a scam artist. It isn't unusual for some to say "I wish I had heard your program before I gave money to that contractor, or bought that annuity, or accepted a free medical device I really didn't need, or actually believed that the guy I met on the internet was in love with me". These are some of the actual things someone has said to me.

Seniors are being targeted because they are thought to have money available. Older consumers may be less technologically savvy and may not understand how much personal information is available about us in the public and in cyberspace. They are being inundated with phone calls that they cannot control. Scammers are now extensively spoofing their caller IDs to make those they call believe they are calling from a place that fits in with their intended scam, such as the local police, the IRS, a charity, Microsoft, and any number of legitimate businesses. Until I tell them in my presentations that they can no longer rely on their phone's caller ID, many in my audience are astonished. I have had my own name and number appear in my caller ID and it is certainly obvious that I hadn't called myself. Scammers have used my name and phone number to call intended targets. I became aware of this when I received a call from someone I did not know and had not called who asked me why I had phoned her. She indicated that she was returning my call to the number that showed on her caller ID, because no message was left.

Imposter scams are everywhere. Like many other seniors, I've received calls involving the tech support scam, the federal grant scam, charity scams, and sweepstakes and lottery scams, among others. I particularly want to emphasize the IRS scams which are quite prevalent at this time of year. Having never fallen for any, I often reflect on how I may have become so popular on the scammer's "mooch lists". It could be that there is a contest among the scammer crowd to see who can get Mary Bach. A man in Syria sent me a Facebook message telling me he wanted to marry me. I assure you, my husband, Len, of 51 years, who has accompanied me today, might object to that! He has answered the phone to hear the jury duty scam and the grandparents scam, among others. The bottom line is that all of these scams are all about money, the potential victim's money, and that is why education and vigilance are imperative. When people understand, they will hang up the phone. At many of my events I always give my audience members permission to be rude! AARP does not want anyone to fall for a telephone line.

AARP has pioneered a nationwide program addressing scam awareness called the Fraud Watch Network. Consumers of all ages can sign up at "aarp.org/fraudwatchnetwork" to receive fraud alerts. It is free of charge and no membership is required. People without computers can sign up to receive alerts by postal mail. Pennsylvania AARP is quite proud that our AARP Consumer Issues Task Force leads all other states in the Nation in recruiting members to join the Fraud Watch Network. Scam prevention and avoidance is our mission and is an essential element in our team's DNA.

AARP sponsored a Hackathon contest here in Washington, DC challenging student teams from prestigious area universities to come up with ideas to help prevent or stop scams. The innovative ideas that were proposed by these students, if implemented, would help stop robo-calling scams and caller ID spoofing, among others. The solutions to stop burgeoning advanced technology scamming must create and use the same technology to work for consumers to end such scamming.

I thank you all again for the opportunity to be here today as someone in the trenches, day to day, trying to make a difference in helping to diminish or eliminate the number of people being victimized by scams or fraud. I like to think that while we can list many of those who have been scammed by their reported acts, that I and my task force are enabling many more that could have been taken, to not be on that list. I welcome your questions.

Prepared Statement of Adrienne Omansky, Founder, Stop Senior Scams Acting Program, Los Angeles, California

Good afternoon Senators, fellow testifiers and guests. Thank you Senator Collins and Senator Casey for inviting me to this important hearing. I am Adrienne Omansky, founder of the Stop Senior Scams℠ acting program. It is an honor to be here to provide testimony on how my program has had an impact on stopping senior scams.

I am a retired teacher of thirty-eight years with the Los Angeles Unified School District. As a teacher of programs for older adults and adults with disabilities, I taught classes in health and fitness and a unique class that I developed in training older adults in commercial acting. In my role as a teacher, I was in a position to hear my students' concerns and one day, over coffee, the conversation led to the subject of scams that they have experienced. Soon, the seniors in the acting class were excited about using their acting skills to educate their peers. It was 2009, and the Stop Senior Scams℠ acting program was born.

The school district embraced our new education program and was especially supportive when we collaborated with several Los Angeles City council members to designate May 15 as Senior Fraud Awareness Day in the city.

In 2015, our school district eliminated all the programs for older adults and our Stop Senior Scams℠ acting program was in jeopardy. We were able to continue as a total volunteer group with the help of our community partners. We were assisted with transportation needs and rehearsal space from the City of Los Angeles. Senior Medicare Patrol and the Federal Trade Commission provided us with educational materials and our program continued.

In the last few years, we have grown and have performed in about thirty venues per year, from a small veterans group, to the convention center with over 1,000 seniors. We have 26 skits in our repertoire. We always include the Medicare, IRS and "I Won a Prize" skits. In every venue, the seniors have experienced many of the same scams, including the IRS and grandparents scams. One of our own cast members. Janey, was a victim of an insidious form of the grandparents scam. The scammer got information from her facebook page and threatened to kill her granddaughter if she didn't send the money being demanded. Janey sent the money. She felt empowered by telling her story to other seniors.

Our program is always evolving, changing, adding and creating. We have help in crafting our skits from a professional theater and performance arts center. Although we use many aspects of theater in our skits including puppets, this is not enough to educate our audience. We collaborate with professional organizations to make sure our information is accurate.

After each skit, our former judge Francine Lyles, or one of our educators, explains the scam to the audience. The finale of the program includes all cast members singing the "Just Hang Up" song and each actor steps forward and tells the audience if they were a victim or target of a scam. At the conclusion of the program the audience is asked to fill out a comment card to tell us what they liked or make suggestions. Bookmarks from Senior Medicare Patrol and the Federal Trade Commission are always given out. In addition, materials are available from the city and county district attorneys' offices.

We often meet people that we cannot forget. The three 90 plus year old veterans who were victims of the same scams. The 99 year old man with the red beret. When he was asked if he enjoyed the program, he said he unexpectedly learned a lot. He came to the center to meet a younger woman. Then there was the young man who brought his grandmother to the senior center because she was about to send money to get back her drivers license. They both approached me with a letter that indicated that she could get her drivers license reinstated if she would send a large sum of money to the address on the letter. To assure her that it was a scam, I told them to go to the Department of Motor Vehicles and have them look at the letter. The lady seemed very upset with her grandson and very embarrassed. I assured her that we were all in the same boat and there were others who have been scammed out of money from a similar letter. They returned two hours later, when our program was over and told me that the letter was a scam. I saw the relief on her face as she joined our other seniors in a post performance discussion. Last year, I met a lady who was shedding tears during our performance. She was sitting next to me. She confided in me that she wished she had seen our program a week earlier. She lost a large sum of money on a "vacation" scam. She was saving her money to surprise her husband with a cruise to celebrate their 60th wedding anniversary. I asked if she would tell her story to our audience. She got up and I stood beside her. The audience was quiet, all eyes on her. She gave the scammer her credit card number over the phone to pay in full for this trip and he took $500 out of her checking

account. There was no cruise. She told everyone that she trusted the young man who told her that she sounded just like his granny.

Our audience members often tell us what they learned from our program.

What have we learned from them?

We have learned that:

- Scams are under-reported because seniors sometimes do not know where to report them, are ashamed of reporting them, and sometimes think it just will not help.
- They are embarrassed to tell their family members, including their spouses. They are sometimes afraid to tell law enforcement.
- They are more likely to tell their peers then anyone else.
- Sometimes seniors do not like professional fraud prevention programs because they often feel condescended.
- Seniors who live in assisted living facilities are particularly vulnerable to scams because they are lonely and they want to win money to help their children or grandchildren.
- Seniors who have been scammed have emotional scars.
- Anyone can be a victim, regardless of education, race, gender, national origin, or social economic background.
- Seniors are the ones to stop senior scams.
- Theater is a wonderful platform to educate.
- Peer-to-peer education works!

The peer to peer model provides a comfortable and safe environment where they can identify with people who have similar life experiences, both as targets and as victims of scams.

The people who are disseminating the information are non-judgemental. This gives the seniors in the audience the opportunity to open up and honestly share their own experiences.

The thread throughout our peer to peer presentation is that “only you and I can prevent senior scams.” We are all in this together!

○