AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–175

STOPPING SENIOR SCAMS: DEVELOPMENTS IN FINANCIAL FRAUD AFFECTING SENIORS

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING

UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

WASHINGTON, DC

FEBRUARY 15, 2017

Serial No. 115–1

Printed for the use of the Special Committee on Aging

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

U.S. GOVERNMENT PUBLISHING OFFICE

26–817 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SPECIAL COMMITTEE ON AGING

SUSAN M. COLLINS, *Chairman*

ORRIN 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
SHELDON WHITEHOUSE, Rhode Island
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
JOE DONNELLY Indiana
ELIZABETH WARREN, Massachusetts
CATHERINE CORTEZ MASTO, Nevada

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

CONTENTS

	Page
Opening Statement of Chairman Susan M. Collins	1
Prepared Statement	36
Statement of Ranking Member Robert P. Casey Jr.	3
Prepared Statement	37

PANEL OF WITNESSES

Phillip Hatch, IRS Impersonation Scam Victim, Portland, ME	6
Timothy P. Camus, Deputy Inspector General for Investigations, Treasury Inspector General for Tax Administration, Washington, DC	7
Lois Greisman, Associate Director, Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission,Washington, DC	9
Diane A. Menio, Executive Director, Center for Advocacy for the Rights & Interests of the Elderly, Philadelphia, PA	10

APPENDIX

PREPARED WITNESS STATEMENTS

Phillip Hatch, IRS Impersonation Scam Victim, Portland, ME	38
Timothy P. Camus, Deputy Inspector General for Investigations, Treasury Inspector General for Tax Administration, Washington, DC	39
Lois Greisman, Associate Director, Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission, Washington, DC	52
Diane A. Menio, Executive Director, Center for Advocacy for the Rights & Interests of the Elderly, Philadelphia, PA	74

ADDITIONAL STATEMENTS FOR THE RECORD

Endorsement letters submitted by Senator Collins	82

STOPPING SENIOR SCAMS: DEVELOPMENTS IN FINANCIAL FRAUD AFFECTING SENIORS

WEDNESDAY, FEBRUARY 15, 2017

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

The Committee met, pursuant to notice, at 2:32 p.m., in Room SD–562, Dirksen Senate Office Building, Hon. Susan Collins (Chairman of the Committee) presiding.

Present: Senators Collins, Flake, Tillis, Rubio, Casey, Gillibrand, Blumenthal, Donnelly, Warren, and Cortez Masto.

OPENING STATEMENT OF SENATOR SUSAN M. COLLINS, CHAIRMAN

Chairman COLLINS. Good afternoon. That was to wake all of you up.

[Laughter.]

I am pleased to welcome both new and returning members to the Committee, and I am delighted that my good friend Senator Casey will be serving as the Committee's new Ranking Member during this Congress. I want to specifically welcome Senator Catherine Cortez Masto from the great State of Nevada to the Committee. We look forward to having you join our work. And, of course, it is wonderful to welcome back Senator Gillibrand who has been so committed to this issue, and the other issues that we have explored as well.

Speaking of Senator Gillibrand, I understand that her son Theo is here today. He is doing a special class project, so he got an excused absence to be at our hearing today for the project that he is doing, and I know that is going to be a very interesting project.

My apologies also that this hearing had to be delayed from when it was first scheduled on February 1st due to a long series of votes on the Senate floor.

During this Congress, this Committee will continue its focus on three major issues:

First, retirement security. We want to make sure that our seniors have sufficient resources so they do not outlive their savings or find that their golden years end in poverty.

Second, biomedical research investments for diseases like Alzheimer's and diabetes that disproportionately affect seniors.

And, third, financial schemes and other scams targeting older Americans, and that is the subject of today's hearing.

Last summer, an 81-year-old constituent came into my office in Portland, Maine, with an alarming story of deception and cruelty.

A con artist claiming to be an IRS agent had just cheated him out of $8,000, and he narrowly avoided losing $15,000 more.

After reporting the crime to the local police, my constituent, Philip Hatch, and his son came into my office. My staff gave him a copy of the Fraud Book that this Committee produced last year as well as a special postcard that we created with tips on how to avoid scams. Mr. Hatch told us that the tactics described in the materials provided were exactly those that were used by the scammer. If only he had received that information sooner, he might have recognized the scam and avoided losing his hard-earned savings.

Mr. Hatch was very willing to testify today and to share his story, but health issues prevent him from traveling. Instead, he graciously and courageously provided a video in order to share his experience, and we will see that video in a moment.

This episode demonstrates two important points.

First, the criminals who prey on our seniors are relentless. They will harass seniors over and over again until they have drained every penny from their life savings.

Second, this Committee's longstanding dedication to fighting fraud against seniors is raising awareness and prompting enforcement actions that are making a real difference. We must redouble our efforts to educate seniors, their families, and their caregivers.

The stakes are extremely high. According to the Government Accountability Office, America's seniors lose a staggering $2.9 billion each year to an ever-growing array of financial exploitation schemes and scams.

Today's hearing coincides with the release of our Committee's 2017 Fraud Book. Like the book that we published last year, it lists the top 10 scams being perpetrated against seniors, along with information on how to recognize, avoid, and report them. In both years, the IRS Impersonation Scam was the leading offender.

These lists reflect the calls made to our Committee's toll-free hotline. In 2015, hotline staff fielded more than 1,100 calls. Last year, the hotline's call volume doubled to more than 2,200 calls. It is clear that our efforts are raising public awareness, and more important, our efforts are producing real results.

I look forward this morning to the testimony of the Treasury Inspector General for Tax Administration's office on recent evolutions in the IRS imposter scam, such as the demand for payment in iTunes gift cards, to which Mr. Hatch and many others have fallen victim. Raising awareness about the IRS scam is particularly timely, as we are in the midst of tax filing season.

Last May, thanks to the work of our hotline investigators, the IG arrested five individuals in connection with the IRS imposter scam. Federal authorities believe that these suspects stole almost $3 million from more than 1,200 victims. In October, 56 individuals and 5 call centers in India were indicted in another important case. In addition to producing criminal charges, these efforts are making it more difficult for criminals to find victims.

I also look forward to hearing from the Federal Trade Commission on other scams that are targeting our seniors, such as those involving grants, counterfeit checks, and romance schemes, which are particularly timely with yesterday being Valentine's Day.

As our 2017 Fraud Book makes clear, while we are certainly making progress, far too many victims are still losing money and often their retirement savings. Law enforcement, consumer advocates, Area Agencies on Aging, AARP, and financial institutions play vital roles, but alert citizens are still our first and best line of defense. I am proud of our Committee's work on this crucial issue to help seniors become more aware and more informed and to put criminals on notice that they will be stopped and brought to justice.

I now am very pleased to turn to our new Ranking Member, 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 your leadership and for convening this hearing, the first hearing of the Committee on Aging, the Special Committee on Aging, for the 115th Congress to discuss senior scams, as she just outlined.

Also, I want to thank her for working with me to address issues impacting older Americans even before the start of this Congress.

I would also like to welcome new members of the Committee. I know right now we have Senator Cortez Masto here—we are grateful that she is with us—and, of course, Senator Gillibrand who has been with the Committee for a number of years. We are grateful for that help, especially on these critically important issues for our families.

The Aging Committee has historically been a committee that fosters both collaboration and bipartisanship on issues facing older Americans, and that was again abundantly clear by the voice vote we held off of the Senate floor 2 weeks ago to approve the Committee budget and the Committee rules. And I think I was late for that hearing, but——

Chairman COLLINS. I was not going to mention that.

Senator CASEY [continuing]. Somehow my voice got recorded. But I want to thank the Chairman for that.

It is my sincere hope that that will continue, and I am sure that it will. The future of key programs for older Americans like Medicare, Medicaid, and others is also critically important to the agenda of this Committee. We have a responsibility, I believe, to protect these vital programs for older Americans.

Today we have the opportunity to hear from experts who will give us testimony on the challenging issue of combating fraud and scams, which, of course, target older Americans—in effect, older Americans as well as their families. Experts testifying today include Diane Menio from Pennsylvania, from a senior advocacy organization that I have worked with over many years, CARIE, and I will talk more about Diane in a moment. But I want to thank her and her organization's work for what you have done for years to help those who are potential victims of these kinds of scams.

I am also pleased to have joined Senator Collins in releasing a Committee report detailing the top 10 scams targeting our Nation's seniors that you saw a moment ago. The report is based upon the experiences of more than 2,200 individuals who contacted the Com-

mittee's Fraud Hotline over the past year. It will inform the work of this Committee going forward.

I was also happy to join with the Chairman in reintroducing the Senior$afe Act last week. This important legislation both encourages financial institutions to disclose suspected exploitation of seniors when they see it and protects them from being sued for making these reports if they have appropriately trained their staffs and made good-faith reports.

In the Commonwealth of Pennsylvania, more than one in six residents is 65 years or older. In 2015, 22,000 cases of suspected elder abuse and neglect were reported to the Pennsylvania Department of Aging's protective services program.

That is why last spring I held a field hearing in Wilkes-Barre, Pennsylvania, to hear directly from constituents—both those affected by scams and those trying to prevent these scams. Just by way of example, a constituent from Kingston Township told the heartbreaking story of a scam artist attempting to steal the identity and use the credit cards of her husband of 43 years after his death. The Luzerne County District Attorney highlighted the most common type of scam happening today, at least in that area: the sweepstakes or lottery scam. Victims are promised lottery winnings if they just pay often sizable so-called taxes and fees up front. The district attorney recalled one older victim being scammed out of $85,000 in the hope of retrieving $1 million in fake lottery winnings.

While experts struggle to estimate the total financial impact of scams targeting seniors, mainly because it is so underreported, they know that it adds up to nearly $3 billion a year in lost savings—and potentially billions more. It is not just money that is lost in these scams. It is older Americans' sense of security and financial independence. It is outrageous that people who have worked very hard all their lives are being targeted for their nest eggs when they are at their most vulnerable. And it is wrong that seniors still feel afraid to report these schemes. They should not be embarrassed or ashamed. They should know that we have their backs and we are here to help them fight back.

That is why enforcement is such a critical part of this discussion. While it may not be easy to track down these increasingly sophisticated scammers and their domestic and international networks and hold them accountable, we must do so for the safety and security of our parents and grandparents.

Recently, Senator Collins and I applauded the Federal Trade Commission and the Justice Department settlement with Western Union in which the company admitted to criminal anti-money-laundering violations that have disproportionately affected aging Americans. This settlement, $586 million in the settlement, will be used to compensate victims of fraud where Western Union agents were complicit in the scams.

But there is more work to do. We will continue to use the spotlight of this Committee to both help consumers understand the threat and highlight the need for action. It is for this reason that I will continue to fight to ensure that the Consumer Financial Protection Bureau has the resources that it needs. The CFPB houses the only Federal office solely focused on sharing financial informa-

tion with seniors and educating seniors about how to prevent becoming the victim of fraud. Until recently, this office was led by former Pennsylvania Secretary of Aging, Nora Dowd Eisenhower, who is in the first row at our hearing today.

We also need to help keep up the fight to ensure that the Affordable Care Act fraud and abuse provisions are in place. We know that the Government has realized a record-breaking $10.7 billion in recovery of health care fraud in the last 3 years, having new tools that increased Federal sentencing guidelines for health care fraud and on from there.

We also know that proposals that I will oppose, like block-granting Medicaid, could present States with real challenges when it comes to addressing waste, fraud, and abuse in programs.

Finally, in order to continue the good work of the witnesses here today, as well as others, and to support our colleagues in other parts of the Government, the Social Security Administration and other departments, in maintaining a skilled workforce, I am seriously concerned about the impact of the Federal hiring freeze and how that will affect middle-class families.

So I look forward to hearing from our witnesses, and I again want to thank our Chairman for gathering us today on this important topic.

Chairman COLLINS. Thank you very much, Senator Casey.

I want to welcome another new member of our Committee, Senator Marco Rubio. Senator Rubio represents the State with the highest percentage of senior citizens. I represent the State with the oldest median age. That is because a lot of my seniors go to Florida, though they tend to spend exactly 6 months and 1 day there. I am not quite sure, but I have a feeling it has to do with taxes. But it is great to have you as a member of the Committee.

And I want to welcome back Senator Warren, who was here briefly and I am sure will be returning as well. We will now turn to our panel of witnesses.

First, we are going to view a brief video from Mr. Philip Hatch. He is from Portland, Maine, and he will share his personal experience dealing with the IRS impersonators that I mentioned in my opening statement.

Next we will hear from Tim Camus. He is the Deputy Inspector General for Investigations at the U.S. Treasury Department's Office of Inspector General for Tax Administration. That may be one of the longest titles of any witness that we have ever had. But his office has done extraordinary work, and I want to thank him.

Next we will welcome back to the Committee Lois Greisman, who is the Associate Director of the Division of Marketing Practices at the Bureau of Consumer Protection at the Federal Trade Commission, better known as the FTC.

And Senator Casey has already introduced our final witness for the day, Diane Menio, and we are very happy to have her here, too. Menio. Did I get it right that time? Thank you.

I want to thank you all for joining us, and we will now start with the video.

STATEMENT OF PHILIP HATCH, IRS IMPERSONATION SCAM VICTIM, PORTLAND, ME (BY VIDEO)

Mr. HATCH. My name is Philip Hatch. I am 81 years old and I am from Portland, Maine, born and raised.

I received a telephone call. I answered the phone, and the man said he was a representative from the Internal Revenue Service. I said, "What can I do to help you?" He said, "Well, we have gone through the records, and there has been a mistake here on your returns, and you owe us $5,988 and some odd cents." So I said, "Fine. Tell me who I make the check out to and where do I mail it?" He said, "Well, we cannot do that. We have a warrant out for your arrest, and the marshals will be in your house within an hour." And I said, "Well, what would you like me to do to help resolve this?" They said, "You can go to CVS and get those iTunes cards, and just when you come back you can read the numbers off to us." I said, "That does not sound like a very professional way to do it." He said, "Well, it is either that or the marshals are coming. If we can do this, we can tell them not to come."

So I did. I went and got these little iTunes cards, came back, read the numbers off them, and they said, "Okay. Now, you cannot tell anybody about this." I said, "What do you mean I can't tell anybody about this? I am going to tell my guy that makes up my tax returns. I am a little mad at him." You know, I said, "He made a mistake." He said, "Well, no, do not do that. Everything will be taken care of."

This started at 4:00 in the afternoon and went until 8 o'clock at night. They called me the next day, and they said there was mistake. I said, "What do you mean a mistake?" "It wasn't $5,900 something dollars; it was $23,000." They had somebody call me on the regular phone—I am still on my cell phone—who said that he was a Portland police officer and that they had a local warrant out for my arrest. So I put my son on the phone, and he goes, "Who is this?" And they said, "Well, who is this?" And he goes—he gave him a phony name and said he was an FBI agent. And they said, "Whoops." And they hung up, and that was the end of it. But I had already sent in $8,000 to these people.

Being in the military and being—working for the Government, you know, when the Government calls up, you say, "Aye, aye, sir. What do you need? Can I help you? Okay." And maybe if I had not had that background, I would not have been so cooperative. But I got—I was mad, upset that I was taken in. Just give me 5 minutes in a room alone with those people and I would be happy.

All I can say is just be wary, you know? You know, just be careful. And when it comes to someone going after your money, just say, "Listen, I will think about it tonight and you can get back to me tomorrow," and then contact someone and find out. That is the best advice I could do.

Chairman COLLINS. As you can see, this is really outrageous and illustrates the lengths to which these criminals will go. And a lot of times, they do target people who are either isolated or have been in the military—we did a whole hearing on scams that are directed at those who have been in the military—and they will stop at nothing. They kept Mr. Hatch on the phone for 4 hours, from 4:00 p.m. to 8:00 p.m., getting him to go from place to place to buy the

iTunes card, which is a new variation that we are seeing on the IRS imposter scam. And it frightens people when they get a call from someone claiming to be from the IRS. It frightens all of us to get that kind of call. And it has become so sophisticated that these con artists can spoof the number so it looks like—if they have caller ID, it will say "U.S. Treasury." So that makes them think that it is for real. And it just shows that they will stop at nothing.

I would now like to call on our first witness who is actually here with us, Mr. Camus, for his testimony.

STATEMENT OF TIMOTHY P. CAMUS, DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, WASHINGTON, DC

Mr. CAMUS. Thank you, Senator. Chairman Collins, Ranking Member Casey, and members of the Committee, thank you for the opportunity to testify on the topic of financial frauds affecting seniors.

Over the past 3 years, TIGTA has conducted numerous investigations on the issue of IRS-related frauds and scams. Telephone impersonation scams, sweepstakes or lottery scams, and email and phishing scams are among the top 10 fraud schemes used by criminals to target senior citizens. I will highlight two major IRS-related scams we have been investigating.

The first is a telephone impersonation scam in which more than 1.8 million Americans reported to us that they have received unsolicited telephone calls from individuals falsely claiming to be IRS employees.

The second is the so-called sweepstakes or lottery scam, which has reemerged as a significant threat to the integrity of tax administration.

The telephone impersonation scam continues to be one of TIGTA's top priorities. No one is immune from receiving these calls. I have received calls myself.

TIGTA has made numerous arrests in connection with this scam, and we have a number of significant investigations that are still underway. For example, this Committee made a direct referral to TIGTA involving a senior citizen located in Florida who was so frightened by the impersonators that, following their directions, he immediately drove to his local Walmart while remaining on the phone with him. During the drive, he crashed his vehicle and continued on foot in order to obtain a MoneyGram payment as demanded by the impersonators.

TIGTA special agents worked diligently on this referral and ultimately identified five suspects in Miami, Florida. These suspects were arrested by TIGTA special agents for wire fraud and conspiracy to commit wire fraud.

In October 2016, after an extensive 3-year joint investigation, the Department of Justice obtained an indictment on 56 individuals, 24 of whom were located in the United States, and 5 call centers located in India. The investigation identified approximately $272 million of total fraud and thousands of victims involving multiple fraud schemes. This is the largest single law enforcement action to date involving the IRS impersonation scam, and the operation's success is a result of excellent cross-agency collaboration and the

efforts of hundreds of TIGTA employees who participated in this investigation.

In addition, TIGTA has taken numerous other steps to fight this crime. For example, we created a strategy designed to shut down the impersonators' callback numbers. We have also developed an outstanding working relationship with the Federal Trade Commission and the Federal Communications Commission to combat this scam. We have worked with the AARP and the Veterans Administration on public warning messages.

TIGTA has also employed a public awareness campaign. We have recorded five videos that received over 71,000 views, and we have provided approximately 100 print and media interviews resulting in over 4,400 news stories in both large and small media markets, resulting in an estimated 113 million views.

We also worked with the private sector such as Walmart and Apple, who were used in this massive fraud. These companies are now helping us to warn consumers about the scam.

As a result of all of these efforts, the impersonation scam's impact on the public has been significantly reduced. Today there are 92 percent fewer reported calls each week and 93 percent fewer victims reported to us that they paid the scammers money. However, the problem has not gone away entirely, and the volume is starting to come back.

For example, we received on average 1,000 reported calls per week in early January, and our data for last week shows we received over 4,600 calls for the week. I believe sustained investigative efforts and ongoing outreach to ensure people do not become victims in the first place is critical to our success in fighting this scam.

Another fraud scheme, the lottery scam, has continued to target and victimize senior citizens. Its premise is simple: The scammers contact victims to advise them that they have won a lottery or sweepstakes, but first they need to pay a non-existent Federal tax or fee in order to receive the prize. Over the last few years, TIGTA has conducted investigations that have identified over 30 individuals who are responsible for defrauding victims out of millions of dollars. We have obtained some prosecutions, and we are working on others to address this crime.

In summary, we at TIGTA take seriously our mandate to protect American taxpayers and the integrity of the Internal Revenue Service. As such, we plan to provide continuing investigative coverage in this area, and we look forward to our continued collaboration and discussions on ways we can fight these types of frauds and scams in the future.

Chairman Collins, Ranking Member Casey, and members of the Committee, thank you so much for your support and for the opportunity to share my views.

Chairman COLLINS. Thank you very much.

Ms. Greisman.

STATEMENT OF LOIS GREISMAN, ASSOCIATE DIRECTOR, DIVISION OF MARKETING PRACTICES, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, WASHINGTON, DC

Ms. GREISMAN. Thank you, Chairman Collins, Ranking Member Casey, and members of the Committee. I am very happy to appear before you again to discuss the FTC's broad efforts to protect seniors against fraud, which is a critical part of its consumer protection mission.

These efforts are driven through the FTC's law enforcement work, its coordination with U.S. and international partners, and, with a tremendous emphasis, its education and outreach initiatives.

First, just a quick overview. As you know, the population of older Americans is growing rapidly. By 2030, more than one-fifth of U.S. residents will be over age 65.

Now, throughout our law enforcement work, we train a deliberate eye on whether fraudsters are targeting specific consumer populations and, in particular, whether they are targeting seniors. We do see that certain types of fraud, such as Medicare imposter scams, deceptive pitches for medical alert devices, brain training programs to treat cognitive impairments such as Alzheimer's, or supplements to address or eliminate joint pain, all may well be directed specifically to seniors. In other areas, such as the technical support scam, where scammers impersonate, for example, Dell or Microsoft and lead you to believe that your computer is in dire straits and that only they have the remedy to fix it, we do think seniors may be disproportionately impacted. And with TIGTA, and as Deputy Inspector Camus has just indicated, we have strong partners in our work and particularly in combating the IRS imposter scam.

But as a practical matter, scammers care little about their victims' age. As a result, we see seniors impacted across the entire spectrum of our consumer protection work, from investment in business opportunity frauds to bogus health care products to time share resales frauds. I want to take a moment to highlight, as Ranking Member Casey referred to, the recent $586 million settlement with Western Union. A good many iterations of fraud flowed through Western Union's money transfer system, but we know, based on the investigation, that lottery scams, so-called emergency scams such as the grandparents scam, and the online dating or romance scams were well represented among the complaints the company received, and we know that these types of scams often target and impact older consumers.

In addition to the more than half-billion-dollar settlement, the FTC's order requires Western Union to implement a comprehensive anti-fraud program that, among other things, will require suspension or termination of problematic agents under certain requirements. And as you mentioned, the Department of Justice entered into a deferred prosecution agreement with the company at the same time.

Not only has the FTC proceeded against money transfers, this morning we announced a settlement with a Florida man and his company that allegedly helped telemarketers in India dupe con-

sumers in the U.S. into paying hundreds or even thousands of dollars for taxes they did not owe. These telemarketers, as we heard from Mr. Hatch, often pretended to be from the IRS or in this case from another Government agency that had grant money to dole out, and told consumers to pay via MoneyGram or Western Union.

The defendants with whom we settled were the U.S.-based entities that orchestrated having runners literally driving up and down the Florida coast to various retail stores to collect the money transfers before consumers realized they had been scammed and could take some action.

And as you know, FTC law enforcement regularly collaborates with our partners here, State and Federal, as well as internationally, and for these purposes, I want to simply note that we and our colleagues have spent considerable time working with law enforcement and other stakeholders here and in India to curb illegal telemarketing hitting the U.S.

Finally, we continue to improve upon and build out our Pass It On education effort. I am sure you are familiar with this. We have shared it with you many times. It is aimed at active adults, and this is our signature initiative. It reaches seniors in social clubs, libraries, senior centers, veterans facilities, and we recently added a new video about how an imposter scam harmed a retired teacher.

We also recently posted another new video about the Pass It On campaign itself, highlighting how important it is for an older consumer to be the one who helps friends and families to avoid being victimized. We continue to use these resources and to promote them with our State and Federal partners.

In sum, through aggressive law enforcement, strategic policy initiatives, and innovative consumer education, we will continue to tackle scammers that exploit older consumers.

I look forward to your questions. Thank you.

Chairman COLLINS. Thank you very much.

Ms. Menio.

STATEMENT OF DIANE A. MENIO, EXECUTIVE DIRECTOR, CENTER FOR ADVOCACY FOR THE RIGHTS & INTERESTS OF THE ELDERLY, PHILADELPHIA, PA

Ms. MENIO. Good afternoon. My name is Diane Menio, and I am the executive director of the Center for Advocacy for the Rights & Interests of the Elderly. I just thought I would say the full name so that you would know why we have a girl's name for a name.

Chairman COLLINS. Thank you.

Ms. MENIO. Thank you, Senator Casey, Chairwoman Collins, and members of the Committee for your interest in financial exploitation, fraud, and scams against the elderly and for the opportunity to present testimony today.

Two weeks ago, Charlotte Kitler from Nanticoke, Pennsylvania, a volunteer in our Pennsylvania Senior Medicare Patrol program, accompanied me here to the hearing. Unfortunately, she could not make it today, but I know she is here in spirit. She was very excited to be at the Senate. And she works very hard with us.

Today I am going to talk about health care fraud. I am also going to talk about abuse, scams, and financial exploitation targeting the

elderly and how CARIE is working to protect seniors across the State of Pennsylvania.

Founded in 1977, CARIE is a nonprofit organization dedicated to improving the quality of life for frail older adults. CARIE works to protect the rights of older adults and promote awareness of their special needs and concerns. In addition, we provide a range of services to help older victims of crime, abuse, and financial exploitation, including a program that helps elder victims through the court process and assists with victim impact statements and Crime Victim's Compensation. In addition, CARIE coordinates Pennsylvania's Senior Medicare Patrol program to help fight Medicare and Medicaid fraud. We have more than 75 retired Medicare beneficiaries who provide that peer education about health care fraud and share information about how to prevent being victimized.

While we talk about the great toll that financial exploitation exacts on its victims, it is important to note that the problem of exploitation impacts many people whether their net worth is in the millions, the thousands, or even the hundreds.

Every day CARIE peer volunteers like Charlotte talk to individuals who have been victims of these horrendous crimes and look for solutions to provide guidance to prevent scams from occurring in the first place.

Additionally, we send out ScamWire alerts that help to identify new threats to the aging community that seek to involve elders in fraud through mailings, email, community meetings, and phone calls. I would like to share just a few stories about cases we hear every day.

Seventy-one-year-old Mary from Philadelphia was contacted by an individual representing himself as a spokesman for Publishers Clearing House. Mary was told that she had won several hundred thousand dollars but had to pay the taxes on the prize. She initially sent them $200. Then she was contacted again, and they told her that she misunderstood and she needed to send another $2,850 in cash via the United States Postal Service. Mary finally thought better of what she did and filed a police report. She initially admitted to the first mailing, but then after talking to our victim advocate revealed the second amount that she sent. And she told us that she was very embarrassed and that is why she had not reported it right away, and that is why she was only willing to talk about the $200 at first because she felt that that was not so bad. But the extra money made her very embarrassed. So she did, after talking to our victim advocate, talk to the police about that, gave them the information that she was given, the address and the phone number of the person that had called her. But, of course, they could not find that person anymore. Unfortunately, she could not get the money back from the Crime Victim's Assistance Fund because there is a time limit involved with that. We just really need to offer some of these people more security and more ability to resist these crimes.

Gloria, who is 88 and from Delaware County in Pennsylvania, received a phone call from a person claiming to be her grandson. When she questioned why he did not sound like himself, he said he was in an auto accident and the airbag hit his face. So she was scammed out of—it ended up being about $7,000 with the iTunes

cards. Older people do not even know what iTunes card is about, but they are told to go and get these. So this was, again, one that the 2-year period had expired.

On an encouraging note, Mrs. Smith, who is a homebound beneficiary and lives in central Pennsylvania, called us to thank us and to let us know that she received our ScamWire alert in the morning, which was included in her home-delivered meal package. That same afternoon, she received a phone call from a scammer and wanted us to know that she knew not to give out any personal information because of the alert. It is stories like these that keep us at it every day. We have seen many similar cases. You will see many more examples in my testimony, and I could even give you more.

The need to prevent financial exploitation is a national imperative. We know that adults and their families must talk about and plan for possible incapacity as well. For those showing early signs of dementia, this is particularly important, as they may eventually lose all capacity to make decisions. Financial capacity is often the first to go.

We do try to work toward positive change. My time is running out, so I am going to conclude here. We are very pleased at the bipartisan attention to elder fraud that the Committee is working on and the Senior$afe Act which builds on lessons learned from organizations like ours.

Thank you again, and we are very pleased to work with you on this issue and are here for anything you need. Thank you.

Chairman COLLINS. Thank you so much for your testimony.

Mr. Camus, you mentioned the direct referral from our Committee's hotline to your office that resulted in the arrest of five suspects who allegedly were responsible for almost $3 million in schemes that defrauded more than 1,200 victims, and this truly was an appalling case that we passed on to you. The senior citizen was so upset that he crashed his car on the way to the local Walmart to get the debit card. And he was convinced that he was going to be arrested immediately, so he leaves the scene of the crash and walks the rest of the way to Walmart.

We were able to determine that the money was sent and picked up in Minnesota and provided your office with that information, and I really appreciated that you acted on it.

Could you please give us an update on that case since the arrest last May?

Mr. CAMUS. Yes, Senator, I would be proud to. One of the subjects has pled guilty, and he has been sentenced to 2 years in prison, and he has been ordered to pay $98,000 in restitution to multiple victims. The other defendants are going through the various stages of the legal system right now, but we anticipate they, too, will be brought to justice here in the very near future.

Chairman COLLINS. That is great news to hear.

Ms. Greisman, I am also really pleased to hear the FTC has stepped up its efforts, and you mentioned the agreement or the settlement with Western Union that had been made. And I am interested in whether or not that $586 million is going to end up compensating any of the victims. Were you able to trace the money that had been lost? And will some of the victims be compensated?

Ms. GREISMAN. Thank you, Chairman. That is precisely the goal of the settlement. The Department of Justice, pursuant to the two agreements, the two settlements, will be the claims administrator, and they will take it upon them to do their best job to try to reach out to victims and provide redress.

Chairman COLLINS. That is so important because in the vast majority of these cases, once the money has been wired, it is gone forever, and it is very difficult to trace. And that is why I really appreciated not only the settlement with Western Union that is going to lead to some restitution, but the quick work of the Inspector General's Office for Tax Administration that really stopped a fraud in progress. That is the kind of cooperation we need across Government.

One of the things that truly frustrates me about these con artists is that they are very clever and they are always changing their tactics to stay ahead of the consumer education efforts that we organize, as well as law enforcement. And I think we are all making a difference, but the fact is that the calls to our hotline doubled last year to more than 2,200. I am going to bring up a chart which demonstrates why scammers—it is a little hard to read, it is a little busy there—but why they are continuously changing their strategies. Let me explain it since it is a bit busy, as I said.

Between November 2014 and early 2016, the losses per month in the IRS impersonation scam averaged approximately $1 million. That is $1 million lost per month. However, starting in the spring of 2016, the losses per month increased to $2 to $4 million, and I can see Mr. Camus nodding his head in agreement. And it stayed at about that level through the end of last year.

What happened during that time is the scammers made a change and they are no longer using the Walmart debit card as much. They have gone to the iTunes card, which struck me as very strange because I thought you used those to buy records. But perhaps I am out of it.

But, Mr. Camus, I would like you to comment on whether the change in tactics plus the relentlessness that we have heard about from Mr. Hatch where they call again and again and the next day with more demands, has that made scammers more successful in terms of the money they are bringing in, even if the number of victims has declined?

Mr. CAMUS. Yes, we noted in April, Senator, April 2016, that there was a shift to the iTunes card as a method of payment. They also redoubled their efforts on their auto-dialer program, so they are able to make hundreds of thousands of telephone calls in a very short order.

To your point exactly, when the scam first started, it was individuals calling one on one. And then when they shifted to the auto-dialer technology, they were able to blanket individuals with hundreds of thousands of calls, leaving a callback number.

At about the same time, they shifted to the iTunes card, and what we learned in our investigation was the iTunes card makes it very easy for them to flip the money. They are no longer paying middlemen to convert payments into money orders. They are now selling the iTunes cards on a third-party market and then pock-

eting the money immediately. And, also, it is very difficult for law enforcement to trace that transaction.

Chairman COLLINS. Thank you.

Senator Casey.

Senator CASEY. Thanks very much.

Diane, I am going to start with you, and not simply because you are a Pennsylvanian but most especially because of your long work. I mentioned as well in my opening comments the acronym, and I want to put the words behind the acronym. Diane, you have worked for, we will call it, a couple of years——

Ms. MENIO. Yes, just a few.

Senator CASEY. Just a few. I guess I can say decades.

Ms. MENIO. It is 28 years.

[Laughter.]

Senator CASEY. For the Center for Advocacy for the Rights & Interests of the Elderly, so-called CARIE. So we are grateful for that work. One question I had was: How do you coordinate in your work with both State authorities and Federal authorities? Sometimes the most difficult challenge in any investigation is the coordination of it. How do you do that? And is there anything we should know about those issues?

Ms. MENIO. Yes, it sure is challenging sometimes. But in Pennsylvania, we actually have a network of elder abuse task forces that operate in various counties across the State. In Philadelphia, our task force is specifically focused on financial exploitation, and so we have bankers and others at the table.

I think that is one of the best ways to coordinate, is to actually know these people, to be able to sit around the table and talk about the problem. Sometimes we do case reviews, so, you know, you get to talk about how this case got played out through the system and it helps us.

Last year, you know, I know the Committee had a hearing about the drug mules that were being used, and one of the calls about that came into our office about a gentleman who was from Pennsylvania and jailed in Japan. And we were frustrated by that because we started calling everybody we could think of, and we found no help for that family. But, eventually, he did get out.

But when we were at our task force meeting, we talked about that case, and someone from Homeland Security was there, and we shared—they gave us their card and said, "Can we share this"—you know, "Can you share the information about the family?" And so we talked to the family, and we were able to connect them with Homeland Security.

So it is that kind of collaborative work, I think, that is very important because we have to know one another. And reaching out to community groups that are in the community that actually work with older adults, working with law enforcement—I mean, we do this in our health care fraud program as well. It is very important that we can get to the OIG's office, that the FBI is involved, all these other groups so that we can get to the bottom of this. It is not always the same agency. So we try to work in collaboration as much as we can.

Senator CASEY. I want to ask as well about the—you mentioned health care fraud. The so-called Senior Medicare Patrol, I know you

have worked very hard with that patrol. We are having a big debate here about the Affordable Care Act, and this is one area where there is a very strong set of numbers that aligns with the progress that has been made over the last couple years in combating Medicare fraud.

To the extent that you can give an opinion on what happens with regard to the ACA, if it were to be repealed, say if it were repealed and not replaced—I know that is a big subject of debate, but just give us your sense of the impact of the Medicare fraud patrol?

Ms. MENIO. Well, there are a number of issues that I think that have impacted health care fraud, you know, uncovering health care fraud, but also just Medicare and other provisions as well that we think are very important, looking at nursing homes and a number of other issues. But one of the things the Affordable Care Act did—and it is sort of related to your last question—is it allowed agencies like CMS, Medicaid, Department of Veterans Affairs, Social Security Administration, and others to data-share, to help them identify criminals who are defrauding. Sometimes, you know, we will get a call—we had a lady in Philadelphia who was a podiatrist, and she went into Chinatown. She was part of that community. And she started basically getting people's Medicare numbers and billing. It turned out she was billing like hundreds of thousands of dollars—it actually was in the millions. At one point she was vacationing in Paris when those bills were submitted.

It is really important, you know, because we had a couple complaints from these beneficiaries, and that is probably not going to rise to the level of a major investigation. But once you start looking at the data, you can see what is happening. And so that is extremely critical. So it is important to see because these criminals are going across programs. They are similar to the other scammers. They are setting up business where it is opportunistic business.

The other thing that I think is important is that they have created—the Affordable Care Act created a Medicare fraud strike force, and I think that costs about $350 million, and so far it has recovered more than $10 billion. So there is real good economic advantage to doing this work, because when they do find these scammers, as I said, a lot of them are very large scale. The one I talked about was probably small compared to some of the large scale. I know in Florida, for instance, there were these groups, these storefronts set up to basically pay Medicare beneficiaries for their Medicare numbers. And so it made these beneficiaries complicit in the fraud. They certainly did not understand what was happening. They were getting $10 or $20 or something like that, but they did not understand what was going on.

So we really need to continue to do this work to make sure that we are combating this stuff. And just sometimes to us, when we are getting the complaints, it seems all too easy, and sometimes the solution seems easy, too. So we really need to make sure that we are looking at how we can make these systems work, and I think the more this—what was provided for in the Affordable Care Act has created some results, and we need to continue doing that.

Senator CASEY. I appreciate that. I am out of time, but will come back. Thanks.

Chairman COLLINS. Thank you.

Senator Rubio.

Senator RUBIO. Thank you, Madam Chair.

I want to continue to build on what you just mentioned about the storefronts, and it is a topic that a lot of people are not aware of. What we have in Florida, what we in South Florida in particular today is an outrageous crisis of Medicare fraud, and let me describe it. And I say this to you as a Cuban American with both deep regret and sometimes shame about this reality. We have literally 50 to 100 individuals, mostly recent arrivals from Cuba, who arrive into the United States, somehow figure out a way to set up a Medicare company. Usually it is a storefront, often just a P.O. box. They then acquire Medicare numbers from a runner, from somebody who works at a hospital, and they begin to bill those Medicare numbers for no services provided. And I am talking about to the tunes of hundreds of thousands of dollars.

I have been flat out told by law enforcement in Florida, in South Florida in particular, that if they do not get greedy and are just willing to steal $200,000 to $300,000 a month, they are probably not going to get caught. They are stealing to the tunes of millions of dollars.

If you look at the list of the top most wanted Medicare fraudsters in America, they are almost entirely from South Florida and almost entirely recent arrivals from the island of Cuba. And when we are about to arrest them—they know they are coming—they leave to Cuba with millions of dollars. It is an outrage. It is grotesque. It has been extensively covered by the press in South Florida. And people may think that seniors are not victims, they are just used. They are victims. Number one, it is helping to further exacerbate the financial troubles of Medicare, and in many cases—you are absolutely right—seniors are being told there is nothing wrong with this, it is legal, just come in, all you got to do is sit down for an interview, give us your Medicare number, and before you know it, it is their account that is being billed for all this amount. And sometimes they get wrapped up in it.

So I hope that we will have a chance to focus on it. We had a chance to discuss it. When I tell people this, they do not believe it can—this is organized crime. In every other sense, it is organized crime, and they are brazen about it. And they laugh about it, because they know they can just leave and are protected if they leave the country.

My mother is a senior—this is why I want to ask you this question—and she has been the target in the past. And I just recalled this as we were having a conversation. After she suffered a stroke in 2011, she is largely home-ridden except she goes to therapy and so forth. She gets a call about taxes she owes, and I know enough about my mom and her finances to know she has not made a lot of money ever, but certainly in the last couple years she has not been employed. She relies almost exclusively on Social Security and small savings.

So we get this number, and we tried to—even though I am in this position of public service, first of all, I did not even know who to call about it at the time. Number two, it is a caller ID, so there is nothing I can do about it. But even if I had been able to lure them into an extensive conversation, I am not sure if I should have

gone to local government or the FBI. There was a little bit of confusion about who to take it to. That is number one.

The second is her caregiver. She has people that come during the day and watch her a little bit, you know, for some time to make sure she is taking her meds. They are often the people answering it. So we have to figure out a way to educate them as well.

And the third, quite frankly, especially in Florida, for a lot of a seniors is a language barrier. My mother speaks English, but her first language is Spanish. That is where she watches the soap operas every night, which I do not fully understand these soap operas and why they are so popular, but she watches them on the Spanish language networks, and a lot of the people that are being targeted for this are also being targeted because of the language barrier.

So I guess in all of that is embedded the following questions: What can we do to improve the awareness of caregivers who might be the people answering the phones when these calls are coming? What can we do to facilitate for them exactly to know who to—like do we recommend that they actually talk to these people, engage them, and try to play detective? Or do we just tell them to hang up and do not deal with them? And the third is: What can we do or should we do to ensure that communities, particularly enclaves of seniors that perhaps are getting the majority of their news and information in a second language like Spanish, that we are doing enough to inform them about these scams and these things that are occurring?

Ms. MENIO. Yeah, I think that the public education is critical. I do think that another issue you might be interested in in the future is looking at why people become subject to scams. You know, we talk about people with dementia, but there is also an issue around financial capacity. Someone may be able to function very well in their life, but their ability to manage finances goes down. And one of the reasons older adults are targeted so often is because they are the ones who are at home and answer the phone. And they might be lonely. And these guys, not only do they come up with the latest best scams, but they also know how to engage people and become their friends. So it is very challenging—I say that because it is very challenging, even when we are doing the education, to get people to pull back from this.

When you talk about the caregivers, the caregivers certainly should be educated about this as well, because they are on the front lines and they will see this happening. I will, though, caution that sometimes we do see caregivers being the exploiters as well. So it is really important for families to be vigilant about this.

We certainly also deal with people with limited English as well. One time we did a presentation in Chinatown, and I think it was simultaneously translated into about eight different languages so that people could get that information. So we try to do as much as we can to reach people and to also train gatekeepers in those communities so that, you know, if it is a Spanish-speaking community, we can train people in that community to take that message to individuals, those people who are going into the home, for instance, who are working in the housing sites. We have housing coordinators who are working with people individually.

So that is where—and we have had scams—we had a scam by somebody telling them they were the cable company. It happened in senior housing throughout the city. And so we were able through that—and one of them was at a housing site where most of the people speak Spanish, and that is where we actually were able to tackle the problem because they got it——

Senator RUBIO. And I know I am out of time. Just a suggestion. We may want to talk to the two primary Spanish language networks about public service announcements as part of their FCC license. I think it would be really useful, especially for the programming that is geared towards an older audience.

Ms. MENIO. And we have been able to get those on our local Spanish language stations.

Senator RUBIO. Good.

Chairman COLLINS. Thank you very much, Senator Rubio. As you were talking, I was thinking that we should get this postcard translated into Spanish as well so that——

Senator RUBIO. Do you want me to do it? I will do it. I can translate it.

[Laughter.]

I even know how to do the accents.

Chairman COLLINS. I have no doubt of that.

Senator RUBIO. We will call you "Susana."

Chairman COLLINS. And I love the idea of including it with Meals on Wheels because that would reach a lot of homebound seniors. So that is something we can look at also.

Senator Gillibrand.

Senator GILLIBRAND. Thank you, Madam Chairwoman, and thank you, Mr. Ranking Member. This is such a vital hearing. You know, I have traveled around New York State asking community centers and senior centers, you know, "Have you been affected?" And, overwhelmingly, almost every hand in the room is raised, because someone has gotten the IRS scam, someone has gotten the grandparent scam, somebody has gotten the sweepstakes scam. And it is heartbreaking, and some of these seniors have lost tens of thousands of dollars. And there is no protection for them, so I have three sets of questions.

First, what should we do as the Senate Committee to—all of you have said, yes, there must be public education. How must there be public education? What legislation should we write about how to educate all seniors about these scams? Specifically, how do we reach all seniors in this country?

Number two, every one of these scams has public participation on some level. The CVS counter that sells the iTunes card, the Target that sells the iTunes card, the credit union, the bank—thank goodness one New York woman, she went to her bank to take out $5,000 to pay the IRS scam, and someone sitting outside waiting for her to bring the money, and the teller so smartly says, "Ma'am, you look so nervous. Are you okay?" And she is like, "No. I have got the IRS on the phone, and I have to give them the money right now." The woman was smart enough to say, "Give me the phone," hung it up, said that the IRS will never call you.

Should we not be having conversations directly with any place you can purchase an iTunes card? Shouldn't there be a notice that

is on every cash register, if someone buys an iTunes card, please confirm it is to purchase an iTunes card for music, or for a video game, it is not to give to the IRS? Why aren't we posting at every vendor that sells iTunes? Every bank, every teller should be trained on this. I do not think we are doing enough to prevent these horrible crimes from happening.

And all of you have said these are significant criminal networks. I have heard some are run by the Russian mob, for God's sakes. Like if we knew massive criminal networks were targeting our seniors, our families, I would think we would be doing much more than we are doing. But for some reason, we are not taking this as seriously as we should. It is, oh, these seniors are being duped, the money is gone. Well, if we had some huge mob cartel bringing drugs into this country, we would have Federal action. We would be sending money to address it. And I do not feel like we are doing that.

And the degree of the scam is much bigger than we have even disclosed. We only have what has been reported. But we know 40 percent is not even reported because it is so embarrassing. This happened to my aunt. She got the IRS scam. She sent the money. She never told my mother who does all her finances. She was so embarrassed. So we are not even getting the full report.

So from each of you, I would like to know what you recommend to us to prevent this from warning various parties that are involved in these scams unwittingly, the people who sell the iTunes cards, the banks. I have a senior who went to her bank and took out an advance. And you know what the bank is doing to her now? Charging her interest because she cannot pay the money back because it is gone. And no relief from her bank. So this is a problem.

So from each of you, direct recommendations for us.

Mr. CAMUS. Thank you so much, Senator. You are right on target with what we are trying to do. We agree that once the money is gone, it is gone, as the Senator pointed out. Public education is the number one way to combat this. Criminals will continue to go for the vulnerable, in this case senior citizens, as long as they get money.

Senator GILLIBRAND. Specifically, what kind of public education and in what form?

Mr. CAMUS. We send our special agents out, and we look forward to invites for town hall meetings, especially at senior centers, and we have had very good feedback on those. So we think we can penetrate into that segment by actually participating with Members of Congress at various town hall events, and we would be proud to have a special agent come and speak to this very issue. So that is just one idea I would have.

As far as the vendors, right now we are working on a project with Walmart to do exactly as you describe, that is, post placards and train their cashiers, and when somebody comes through with a handful of iTunes cards, that there is some sort of a dialogue that goes on prior to that purchase being consummated: "There is a scam going on. Are you aware of the scam? Have you been told that these iTunes cards are for taxes? If you have, it is a scam."

We have been successful with MoneyGram, for example, that when individuals go on to the MoneyGram kiosk in a CVS, one of

the warnings that pops up early in the transaction is: "If you have been told to pay your taxes with a MoneyGram, you are being scammed. Please stop the transaction."

So we totally agree with you that we have to leverage the retailers and get them to cooperate, and in some cases we have. A recent shift that we have seen is primarily Walmart was being used as the retailer, and now our data is telling us within just this past month that it is now being shifted to Target. So just yesterday, I had one of my executives reach out to Target, and we are going to insist that Target work with us the same way Walmart did.

But for us as a small agency, a small law enforcement agency, we think that every person that we protect is a victory. That is how we view this. It is not just a law enforcement aspect. It is every single person that does not become a victim is a victory. But how do we collectively—to your point, how do we collectively come together and make a bigger impact?

So certainly working with the FTC is something that we have really enjoyed doing, but there is still more that could be done. But I just want to give you the assurance that we are doing a lot behind the scenes.

Ms. GREISMAN. Thank you. I appreciate the opportunity to address the points you raise. It is very serious, and I do not want to have you think in any way that this is not a top priority for the Federal Trade Commission.

In terms of prevention, I would urge each of you, if you do not already use our Pass It On materials—put them up again—these are tested. This is, we think, a very effective way to reach seniors where they are and to provide them with the tools they need so that they are the ones positioned to assist friends and family members not to be victimized. There is a specific piece on IRS imposter scams.

The intermediaries, there are two things we do. One, we sue them. That is what the settlement with Western Union is about. We had a settlement years before with MoneyGram. Through amendments to the telemarketing sales rule, we made illegal wire transfers in connection with telemarketing, and we also prohibited other types of reloadable cards being used. So law enforcement is front and center in terms of the intermediaries.

Also, as Deputy Inspector Camus referred to, we have lots of conversations with Apple, with Walmart, with the trade associations for relevant industry members. The Western Union settlement, like the MoneyGram, imposes specific requirements to make it more likely that the company will intercept and prevent the transfer of money, because as we have all discussed, once it is gone, it is gone. And that is exactly why the scammers are using those types of payment instruments.

So that is where we are. We will continue to work with industry members to get better signage, to get other analytical tools in place so that they can identify where the bad actors are and how the transfers are going forward. Thank you.

Ms. MENIO. I cannot agree more with what you said, but I do want to put a plug in for the Senior$afe Act, which is one thing that you can do. One of the biggest problems we have had with financial institutions is making these reports.

In my written testimony, you will see a story about a lady who was bilked out of $800,000. That was basically everything she had. She was in her 80s, and she thought she was winning the lottery. And so she kept paying money and did not tell her family until it was way too late. And I think it was finally—she and her husband had invested their money with an investment firm for, you know, all their adult life, and her husband had died, and that was their money in the bank. And no one made a report, and eventually the money got transferred to another bank, and she continued to buy these Walmart cards and everything to pay this thing. And, finally, that second bank made a report, but that was after $800,000 was lost.

So we need to do something to make them feel better. I mean, you know, we keep pulling out the Gramm-Leach-Bliley Act and saying, "You can do this. You are covered." But they still are not doing it. And sometimes—I can tell you what happens—in some of the cases that work out well, it is the teller who is making the report. They are not necessarily authorized by the guys at the top, but it is the teller who is coming in and they are seeing all these withdrawals taken. So that gets to your point of training the people who see it happening, the people who are—the tellers at the bank—although we have fewer and fewer of those these days—and the people who are at the stores.

The other thing is that we need to encourage age-friendly services in those institutions. We need to have fraud technology. There is a lot of technology out there these days. I remember sitting in a meeting with the bankers and saying, well, you know, if I am out of town and I use my credit card—like I was somewhere, in Chicago I think, and suddenly my card got shut off. Well, you know, it was legitimate charges, but they shut off my card because they were monitoring it. I said, Why can't you do that for some of these cases? And they are very shy about doing that. They will not do it.

But those technologies really need to be used for this. They need to come into action. And the age-friendly services are also important, to make sure that they have protections, like encouraging them to plan for incapacity, offering age-friendly account features, like having someone who has access to your account. Maybe they cannot take money out, but the daughter, for instance, can get in and monitor online to make sure nothing is going wrong.

And so all of those kinds of things I think can be done. I hope that we can do more to combat this, and we need to—you know, when you talk about education, sometimes it really is just as easy as putting up a sign at the cash register so the person managing that cash register sees somebody buying—an older person, somebody who is 80, 82 years old, buying all these iTunes cards, that is a flag. I cannot imagine why you would not report that. So we need to do exactly what you are saying.

Chairman COLLINS. Thank you.

Senator CORTEZ MASTO.

Senator CORTEZ MASTO. Thank you. I am very excited to be a member of this Committee, so thank you very much. And thank you to all of you for what you do.

I was fortunate to be able to work with the FTC as the Attorney General of Nevada and had great partnership, and many of you we have worked with on so many different levels. This area was important for me as Attorney General. That is why I created a unit in my office to address elder abuse, neglect, and exploitation. Every single one of the scams that you identify here happens in Nevada, and we had some great partners.

I want to talk on a couple of levels, though. The first one is the public education, because to me this is the first step in prevention, and it is so hard to do. It really is. There are many of us that are trying to do our outreach and get out and talk to folks, but it has to be on a constant basis. You cannot just say I am throwing this out there, we will it overnight, and that is done. The education occurs all the time. All the time.

I have been—I always say this—just about to every senior center in Nevada to reach out to our seniors. But it is not just reaching out to seniors. It is reaching out to their caregivers. It is reaching out to family. It is reaching out to service providers. So for my purposes—and this is what I am going to ask with your help—I had put on conferences in the State of Nevada, just bringing people in for the training, for the public education, bringing the experts in to talk about it, how we educate, how we train, and how we constantly get that information out. That is one thing that I would love your help with in Nevada, to continue down that road.

The next one, however, is challenging for me when it comes to law enforcement, and this is a question I have for our law enforcement folks. Given the aging population—in Nevada it is growing, but also we are constantly evolving with technology and technological scams—what additional resources or innovations does law enforcement need to keep up with the financial threats posed to seniors now? And when you talk about it, talk also about how we examine also the money transfer systems, which make it much easier for some of these criminal elements to engage and scam our seniors.

Mr. CAMUS. Just a couple ideas. Thank you, Senator, and we do look forward to working with you in Nevada.

One of the ideas you could come up with would be—there is a 72-hour right of rescission on large transactions, so maybe it could be considered that on any wire transaction, instead of it being rapid and instantaneous, there is some sort of a 72-hour right of rescission, because many of the victims that we spoke to, they realized it, but just a little bit too late. By the time they realized or talked to a family member about being scammed, the money was already gone, and there is no way to get it back. But if we could get that frozen for just a period of time to allow a recognition, a family discussion, or law enforcement to intercede, we might be able to save people a lot of money and save their lives actually.

But as far as some of the other ideas, the challenge for law enforcement is the money moves so quickly and the ability to convince somebody to put their Federal income tax payment on an iTunes card, that is really difficult. As I said in my testimony, we estimate that just through media on our own as a small agency, we believe that we—we had 113 million views, over 100 media interviews, and it is constant with us. We had Apple agree to fund a

pilot program where over the air in CVS stores and other drug stores, the message over the air as they were shopping was, "Do not use Apple iTunes cards to pay public debt. Do not use Apple iTunes cards to pay Government. It does not work that way." And we think that that worked, but it is very, very expensive. That project cost Apple I believe $140,000 to fund that. But it was a pilot.

So if we could get more of that type of cooperation, a fund set up where some of these retailers and companies are required to put aside some money to help educate and continuously educate—because it is so difficult to penetrate. You know, I am not a journalism major, but I am astounded by how difficult it is and how—and I take calls myself at my desk. And just this morning, I took a call from a victim, and they had no idea that there was any such thing as an impersonation scam. And it perplexes me. I am, like, "What more could we all do, what are other things that we can do to try to reach that?"

Senator CORTEZ MASTO. Yeah, and that is why it is constant. The education has to be constant, because people are not really listening. And let me just say one thing as well, and I found this in Nevada. Part of it, too, is when they become victims—and we have heard it here, but they are embarrassed to come forward. They are embarrassed to say that this happened to them. And we have to give them a venue to be able to say it did happen, it is all right, it is happening across this country, to make sure that they are willing to come out and educate themselves and educate others about this type of scam.

Ms. GREISMAN. Thank you, Senator, and we have enjoyed the cooperative relationship with your former office as well.

You mentioned how do we get out into the community. Well, we have had some 33 common-ground conferences throughout the country. One was in Vegas with the help of your former office. There we are working with grassroots members, people from the Chamber of Commerce, legal service providers, obviously the Attorneys General offices, local law enforcement. And the discussions vary nationwide, but a lot of focus is on issues affecting seniors in the community. And we learn from those conferences. We push out our consumer education materials. We will continue to do more on that front.

Money transfer services, well, I would like to sit here and be cautiously optimistic that the near half-billion-dollar settlement with Western Union will squeeze some of the fraud out of that system, and I think it will. It is an order with very rigorous requirements that, if they adhere to them, should make a difference. Of course, if we are squeezing money out of that system, then it is just going to find another path of less resistance to move to.

There is no silver bullet in this. Education has to complement law enforcement, and that is what we are committed to doing. We certainly look forward to working with each and every one of you to build upon what we have been doing.

Senator CORTEZ MASTO. Thank you. And let me just add one final thing. Diane, the Senior Medicare Patrol unit was in my office. It is instrumental. I will always continue to support it. I cannot tell you how many seniors not only were excited to be a part

of it, but we were able to uncover fraud. And I cannot say enough about the journals, the diaries, the health care diaries and journals that we would hand out to individuals. It matters. They really pay attention when you talk about it and when you have their peers talking to them about how we address Medicare fraud and Medicaid fraud, which we handled in my office. It made a difference. So I will continue to support programs and advocacy, so thank you for what you do.

Ms. MENIO. Thank you.

Chairman COLLINS. Thank you, Senator.

Senator Flake.

Senator FLAKE. Thank you, Madam Chair. Thank you. Sorry if I am plowing old ground here, but could you tell me what innovative programs are already out there that the States have come up with for addressing these senior scams? Anybody who wants to start there.

Mr. CAMUS. As far as the States are concerned?

Senator FLAKE. Yes.

Mr. CAMUS. We work with multiple States, and we work with law enforcement agencies, local and other Federal partners. And I am not uniquely aware that any of the States that we are working in have come up with innovative approaches, but I am probably not the one that is best suited to answer that.

Senator FLAKE. All right.

Ms. GREISMAN. Many States have wonderful, robust programs addressing fraud targeting seniors. Many have discrete offices that directly focus on that, and to the extent possible, we work closely with them. I had mentioned earlier our Pass It On materials. We freely distribute those to the States. We urge everyone to put their own name on it. We have no copyright interest in it. We just want to pass on those materials so that they can be used.

Senator FLAKE. Okay.

Ms. MENIO. And can I just add that one of the tools we have at the State level is the Older Adult Protective Services Office, which often gets the first report on these cases. And I just want to say that one of our recommendations is to make sure that those programs are strong enough to do what they need to do.

One of the things that they often lack is forensic accountants, for instance, to be able to actually take on a case and figure out what is happening. So we need more resources in that program. And at the same time, we are aware that the social services block grant funding is under question at this point, and that is the money that often supports those programs at the State level. So, you know, while we need to enhance the funding for those programs, we need to at least maintain the funding for those programs, because they are often the first line. When Senator Rubio asked who to report to, I did not answer his question, but what I meant to say was just report it, it does not really matter, because when you report it to one place, it will get to the right place eventually. And that is what Protective Services does. It is the first line, and it is very helpful to be able to get that person into the system.

Senator FLAKE. Well, thank you, Ms. Menio. You mentioned in your testimony that a beneficiary called to thank you for the timely ScamWire alert she received in her home, and they delivered a

package shortly thereafter. Are there any reoccurring services that seniors use where companies can include these fraud alerts so that they can be delivered more——

Ms. MENIO. Yes. We also distribute those to public libraries, senior centers, senior housing. We distribute them to a large number of places where we know—grocery stores, places where people gather, where older people do business. And the home-delivered meals project that we do is really focused on people that we will not reach by going to a library or a senior center or those kinds of places. It is the people who are homebound and do not get out and would not get that message otherwise. But we are trying to do that through many different public venues.

Senator FLAKE. All right. Thank you, Madam Chair.

Chairman COLLINS. Thank you, Senator Flake.

Before you were here, Ms. Menio mentioned the Senior$afe Act, which you were a cosponsor of in the last Congress and which we have reintroduced. Senator Casey is a cosponsor. And just yesterday, AARP has endorsed that bill along with we have endorsements from Legal Services for the Elderly, the National American Securities Administrators Association, the Conference on State Bank Supervisors, the National Association of Insurance Commissioners, and a wide variety of regulatory groups, and that is one concrete action we could take in this Congress that would really make a difference in empowering those front-line tellers that our witnesses were describing and who can make a real difference in stopping fraud right up front. So I am going to ask unanimous consent that all of those endorsement letters be entered into the record.

[The letters referred to are in the Appendix.]

Chairman COLLINS. Senator Warren.

Senator WARREN. Thank you very much, Madam Chair, and thank you very much for holding this hearing, you and the Ranking Member. And I want to just follow up. I think your point about how better to empower people on the front lines is really important. I just want to look at another aspect of that.

As we know, the con artists who perpetuate IRS impersonation scams, identity theft, and other forms of financial exploitation often target seniors. And when a senior needs to report that they were the victim of fraud, it is frequently the men and women who work in our Government enforcement and consumer protection agencies in Washington and in all 50 States who are on the front lines taking their calls and investigating their cases.

So it seems pretty obvious to me that one easy way to protect America's seniors from fraud is to strengthen that workforce. But instead of staffing up the workforce that cracks down on scammers and fraudsters that hurt our seniors, on his first full day in the Oval Office, President Trump issued an Executive order freezing Federal hiring and starving our enforcement agencies of their most important resource—American workers.

So, Mr. Camus, you are Deputy Inspector General for investigations at the Treasury Inspector General for Tax Administration. Your job is to protect seniors against scammers who pretend that the IRS is calling and trying to collect back taxes. Almost 2 million

people have reported this scam to your office, and these scams have cost Americans more than $54 million. That is a lot of money.

Does a hiring freeze help you achieve your goal of protecting seniors from fraud?

Mr. CAMUS. As you point out, Senator, these are—it is a huge issue, and every one of these victims is a significant challenge on our resources. So, naturally, I have been told I am not allowed to pander for resources at these events, but——

Senator WARREN. Okay. We will let you know if you have crossed the line into pandering here.

[Laughter.]

Mr. CAMUS. I can tell you I am very proud and we are very efficient agency, but certainly this has stretched our agency very thin. We are seeking the exemption in the President's order under a public safety clause, at least for the special agent portion of our workforce.

Senator WARREN. Well, I appreciate that, Mr. Camus. You know, according to testimony from your office back in 2016, "Reduced staffing has affected the IRS' ability to deliver its priority program areas, including customer service and enforcement." Given that your enforcement team is already understaffed, I worry that this kind of hiring freeze is music to criminals' ears.

Now, Mr. Camus, you also work with the Department of Justice to help protect seniors from criminals who are trying to defraud them. Will the hiring freeze help you with the DOJ?

Mr. CAMUS. Again, you know, it is—we are only limited, all of us are only limited by how much resources we have, and we are all very passionate about protecting all Americans, but most especially our most vulnerable. That is why I took the oath to be a law enforcement officer. So it is a challenge. Resources are a challenge on a good day. So any disruption in that is certainly a cause for concern.

I am not sure whether the Internal Revenue Service or the Department of Justice have any exemptions available to them under the order.

Senator WARREN. All right. But if they do not?

Mr. CAMUS. I could not comment. I do not know the impact.

Senator WARREN. You know, I just want to point out we have seen this movie before. A 2011 hiring freeze at the Social Security Administration eliminated 15 percent of the agency's workforce and closed 64 field offices. Ms. Menio, you are the executive director at the Center for Advocacy for the Rights & Interests of the Elderly in Philadelphia.

Can you explain how the 2011 Social Security personnel freeze affected the seniors that your center works with every day?

Ms. MENIO. Well, certainly it takes a lot longer to make an appointment.

Senator WARREN. So increased wait times.

Ms. MENIO. I can tell you that we are—you know, interestingly, the Social Security—I am in downtown Philadelphia, and the Social Security office is in our building. They have the top floor. And the way that it works is no one goes upstairs until the guard lets them go upstairs, so they get the message, "You can send more people up." And that line gets quite long, and people are standing

there with their walkers and their canes and waiting to go upstairs. And so that is something I see every day.

I can also tell you that my staff spends a lot of time when they are helping consumers doing three-way calls because we are not—you know, we like to empower people and work with them, but sometimes it is difficult for them to make that call on their own. So we will sit with them, and they tell me it is 30 minutes to an hour sometimes they are waiting for that call to get through.

We had a client who called us recently from the western part of the State. Her husband died and she was collecting—she wanted to switch her Social Security so she could collect on his account, I believe something like that. And what happened was—and, you know, I think this is illustrative of the short staffing. She got lost in the system. She did not get a check at all for 3 months, and that meant her Medicare Part B was not being paid. And so she did not even have her health care during that time. Eventually, we were able to help her get that back, but, nevertheless, it was a very stressful time for her. It should not have happened that way. It probably took more man-hours from the Social Security office to fix this than it would have taken to help her in the first place. So those are some of the kinds of things we are seeing.

I also know that the Center on Budget and Policy Priorities put out a report, and they said that less than 1 percent of their expenses are spent on overhead. I cannot run my agency on less than 1 percent—I wish I could, to be honest with you, but I cannot. And so that just is not realistic. How can you continue to provide the level of services to this aging population, to many of us who are ready to, you know, go into the Social Security system, into Medicare? We need to be able to get that information as quickly as we can and work with people without going through a lot of red tape and spending hours on the phone and in offices.

Senator WARREN. And I appreciate that. I just want to add a couple of statistics if I can, and then I will quit. Thank you, Madam Chair.

You know, appeals times also go up. She is talking about helping people apply. But the appeals times go up. Almost 20,000 people died waiting for a disability eligibility discussion in fiscal year 2016. You know, with all of these negative consequences, you would at least hope that these freezes save money. But what the data actually show is that they do not save money, that we have a workforce that is just more stressed, more inefficient. You spend more time trying to fix the problems that are broken because you did not solve it early on.

I just want to say I appreciate the work you are doing, and I hope that we can give you better support to do it. Thank you.

Thank you, Madam Chair.

Chairman COLLINS. Thank you.

Senator Tillis.

Senator TILLIS. Thank you, Madam Chair, and thank you all for coming before the Committee and, at least in one case, returning to the Committee.

I have got a more general question. This Committee is intended to provide insights into seniors' abuse, caregiver programs, those sorts of things, over the course of the last 2 years that I was on

it. And then we have had some discussions about legislative proposals here at the Federal level, and we have talked about potential best practices down in the States. But it does not seem to me we have made much progress, so could you give me in any of your opinions, in the capacity before this Committee, of examples of where I should be kinder in my assessment? What kind of progress are we making at the State or Federal level that you think is really moving the ball substantially in the right direction? Mr. Camus, want to start with you?

Mr. CAMUS. One of the biggest challenges I have, Senator, is—and I have been working with staff here—as we investigate crimes, we learn. We learn how they are doing it; we learn how they are shifting. And as Senator Collins pointed out, the criminals are watching every single thing that we do from all over the world, and then they are adapting to what we do. It is literally a cat-and-mouse game, and they will continue to victimize our most vulnerable citizens because they can get money. So any ideas that we have, we are happy to meet with staff and talk about this is how the crime happened, so legislatively, what are some of the areas that could be explored.

One of the things we are excited about is in our investigation through the FTC's help, we started working with the Federal Communications Commission, and what we learned was they have task forces under the U.S. Telecom Consortium that are actually working on technology to block robocalls that are coming in spoofed. And in one pilot, in the IRS——

Senator TILLIS. Not political ones, right? No, I am kidding.

[Laughter.]

Mr. CAMUS. In the robocall area, in a pilot, they were able to block about 2 million spoofed calls that were coming in that could have hit the seniors. How many people would have been victimized by those calls?

And then the other area that we are excited about the technology is there is a trace-back task force as well, and what that will allow us to do as law enforcement is be able to figure out, when the bad guys are calling in from offshore, quickly determine where that call came from and then work with partners offshore to try to get them investigated or taken out of service.

Senator TILLIS. How do we get to a point where we are scaling some of those things to where we are going from kind of a good proof of concept to a pervasive capability that—clearly something like that could have a significant effect on a lot of the nets that are being cast and then capturing seniors and then taking advantage of them. So I think that is more of—we will go down and just get an assessment for why I should feel better about things that we can scale, but give me your read down the panel.

Ms. GREISMAN. Thank you, Senator. I appreciate the opportunity to be here again.

Aggressive continued law enforcement is ongoing, and it is making a dent. It may not be a sustained dent, but you have got—that is not a reason not to do it. I will point again to the recent Western Union settlement, $586 million, with significant injunctive relief requiring the company to change how it does business in terms of fraud prevention.

The recent crackdown by DOJ with TIGTA on entities in the U.S. and in India, targeting U.S. consumers with the IRS imposter scam, those make a difference. We need to figure out how to sustain them and implement them on a more permanent basis.

Mr. Camus just referred to some of the work going on with robocalls. We have been at this for years, and what has happened as a result of it is that new technologies have been developed, they are in the marketplace. One of the first ones was a result of an FTC challenge back, I think, in 2012. These are call-blocking technologies that work. And then there is more great cooperation and coordination among industry and Government to bring these technologies to the forefront and also to develop—though it is not going to happen overnight—caller ID authentication. That will provide a significant tool, technological change that will prevent some of these calls from hitting consumers. So I think there is good reason to be optimistic.

Ms. MENIO. Well, I wish I had some of their answers for you, but we are not on that scale. But I think on a very large scale, in a sense, our Senior Medicare Patrol is a good example of this work, and it is in every State in this country. And I can tell you right now we are working—we had some consumers, some beneficiaries call us about something that we think is a scam, not totally—we are not sure yet, and I am not going to say what it is because it is being investigated right now. But what we were able to do is get on the phone with people from your State and from, I believe—I am not sure if it is Maine or not, but it is one of the New England States—a number of States with our colleagues who are doing the same work we are doing, and we were finding out that the same scam is—or the same situation is happening in each of those places, which made it a lot easier for us to go to the Inspector General with this. And so it is being investigated now. We think it might be a very large scale issue. That is the way—but, again, it gets back to that working in collaboration with other people is so important, because we get two calls, we will say maybe it is a problem, maybe it is not. It sounded fishy, so we definitely wanted to look into it further. But with those two calls, nothing was going to happen when we called the OIG. But once we get our colleagues from other States identifying these problems as well, then that makes a case. And I think something can happen to protect people in the future through that situation.

Senator TILLIS. Well, thank you, and I know that the Chair has put together great proposals for programs that have worked their way through Congress and authorizing maybe additional initiatives that will be helpful. But it really also points to why we have got to get to a regular order appropriations process so that we then have the financial resources behind these programs to scale them and get them implemented, and so that we can come back and start measuring what I think are the results that can come about. A lot of great ideas, a lot of great pilots, a lot of great proofs of concept, a lot of great law enforcement actions that we have just got to scale. And then, also, if I had more time—I am way over now. At the end of the day, most of what we are talking about here are the cure. We have got to work on the prevention side, which means that we have to continue to focus on education, destigmatizing pub-

lic acknowledgment that you have been abused, and doing those kinds of things so that you very early in the cycle of abuse prevent it from ever happening.

Thank you.

Chairman COLLINS. Thank you very much, Senator. I certainly agree with your comments about the appropriations process. I would indicate that, compared to the very first hearing that we held on scams, we have come a long, long ways. Law enforcement has stepped up to the plate, has started aggregating these scams rather than dismissing them because they are only $2,000 here or $3,000 here. And when GAO came out with $2.9 billion annually, I really think that helped, and our hearings helped raise the awareness of the public and the need for aggressive enforcement, the cases that were described earlier today. So I am actually encouraged that we are making progress, but these criminals are relentless and will continue.

Senator TILLIS. Me, too, Madam Chair. I am just mad at the people that do this, and I want them to suffer badly as a result of it, as quickly as possible.

Chairman COLLINS. Well, there is nothing like putting people in jail to be a good deterrent, that is for sure.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Madam Chairwoman, and thank you for having this hearing and your very, very persistent drive to increase the effectiveness of our laws and the enforcement of them. And like my colleague from Nevada, I was State Attorney General for some years—in fact, 20 years—and we established a unit quite a while ago to focus on elder abuse and criminal activity that victimizes them. And I agree as well that education is among the best preventive steps. An ounce of prevention is worth a pound of cure. Recovering money after the fact is very difficult, but it is possible. And educating the bad guys is important, at least as important as educating the good guys, because educating them through deterrence, the Chair is absolutely right that prison time teaches a very valuable lesson.

So with that in mind, I introduced a bill called the "Robert Matava Criminal Victim Abuse Prevention and Restitution Act." It became, with bipartisan support, the Elder Abuse Prevention and Prosecution Act, which was approved by the Judiciary Committee. In fact, it is bipartisan. Senator Grassley and I together lead it, and it would improve the current law in a number of ways. It is now out of Committee. It is on the House floor. We can approve it if we get bipartisan support there; and if our distinguished leadership there puts it on the floor, I am sure it will be approved near unanimously.

It would expand data collection and information sharing to better prevent and respond to elder abuse and exploitation. It would increase training, improve information sharing among agencies, and it would increase penalties for perpetrators of these crimes. So the anger that my colleagues feel could be channeled very positively and effectively against those bad guys by passing this measure, including mandatory forfeiture to deter future offenses.

Everybody here knows that what drives these crimes is money. If you require mandatory forfeiture, it hits them where they live.

And mandatory forfeiture, in fact, will enable more restitution so that we prevent by deterring but we also make people whole, or at least work to make them whole.

So to any of you who would like to answer, do you believe that mandatory forfeiture, restitution, and increased penalties for perpetrators will be effective in deterring future criminal activity? That is the softest ball that anybody has thrown to you in quite a while.

[Laughter.]

Mr. CAMUS. As a career law enforcement man, yes. We work really hard and we dedicate resources to investigate these, and there is nothing like at the end of the day when my agents can go to court and the perpetrator especially picking on our vulnerable citizens gets a significant sentence. So the more that we could punish them and the more that we can rapidly recover any monies that are available—in many cases, there may or may not be assets available—the better for us. So we wholeheartedly agree with increased deterrence through increased penalties.

Ms. GREISMAN. Senator, it is a delightful softball. We are a civil law enforcement agency, so I cannot speak to it. I have to defer to my criminal colleagues. I will say, though, that anything that ramps up deterrence and helps us on the civil side would be greatly appreciated.

Senator BLUMENTHAL. Thank you.

Ms. MENIO. And I would just like to add that I think one of the reasons that elderly are targeted is that oftentimes the perpetrators feel that they are not going to—and I am talking more about that homespun type of financial exploitation that happens. They just think they are going to get away with it, because they do. And so one of the things we are advocating for in Pennsylvania is enhanced sentencing for people who commit crimes against the elderly.

So I think it is very, very important because the other issue that we have often with crimes against the elderly is that if someone does have dementia, oftentimes we are finding that the police are not arresting because that person is not a good witness in court, they are not a good reporter. So we have got to get past that as well. And I can tell you of some horrendous crimes that have been committed against people who are without capacity. And we have got to come up with a system to make sure that there is a reason for people not to do this, that they are going to be a little afraid of taking advantage of the elderly. So thank you for that.

Senator BLUMENTHAL. Thank you all for your support, and thank you for your great work. Thank you, Madam Chair.

Chairman COLLINS. Thank you.

I want to thank all of our witnesses today for your very important contributions, whether it is law enforcement or education or civil actions against those who would rip off some of the most vulnerable citizens in our country, our Nation's seniors.

As we have heard today and as our Committee's new Fraud Book makes clear, criminals are relentless in their pursuit to swindle seniors out of their hard-earned savings. We see infinite varieties of these scams. Once one is closed down, another pops up. I, too, have had those phone calls on my home answering machine in

Bangor, Maine, and I called the IG's office up immediately because I was so excited. I thought I could help entrap one of these criminals, and it turned out that the numbers expire after 3 days. So that by the time I got home for the weekend, the numbers were no good. I was so crushed because I thought I could help bring these people to justice, which is exactly what is the commitment of each and every one of us here.

While much remains to be done, I am proud that this Committee has been just as relentless as the criminals in fighting back against this fraud, and the important work that all of you are doing really contributes to our efforts.

I look forward to continuing to work with our Ranking Member and with our returning and new members of the Committee as we continue this fight in the new Congress. Committee members will have until Friday, February 24th, to submit questions for the record.

As a reminder, at the risk of sounding like one of those late-night infomercials, the Committee's toll-free fraud hotline number is 1–855–303–9470. 1–855–303–9470. The reason I mention that is those 2,300 calls that we got last year enabled us to identify new scams so that we could warn people and come up with tips for avoiding people becoming victims. So we have distributed so many copies of our Fraud Book and our postcard, and we are going to continue those educational and prevention efforts as well.

I would call on our Ranking Member if you have any concluding remarks that you would like to make, Senator Casey.

Senator CASEY. Thank you, Madam Chair. 1–855–303–9470.

[Laughter.]

Thank you for the message. Thanks very much.

Chairman COLLINS. Thank you. This concludes our hearing. It is now adjourned.

[Whereupon, at 4:19 p.m., the Committee was adjourned.]

APPENDIX

Prepared Witness Statements and Questions for the Record

PREPARED STATEMENT OF SENATOR SUSAN M. COLLINS, CHAIRMAN

Good afternoon. I am pleased to welcome both new and returning Members to the Committee, and I am delighted that my good friend, Senator Casey, will serve as the Committee's new Ranking Member. My apologies that this hearing had to be delayed from when it was first scheduled on February 1st due to a long series of votes on the Senate floor.

The Committee will continue its focus on three primary issues this Congress: retirement security; biomedical research investments for diseases like Alzheimer's and diabetes that disproportionately affect seniors; and financial schemes and other scams targeting older Americans—the subject of today's hearing.

Last summer, an 81-year-old constituent came to my office in Portland, Maine, with an alarming story of deception and cruelty. A con artist claiming to be an agent of the Internal Revenue Service had just cheated him out of $8,000. He narrowly avoided losing $15,000 more.

After reporting the crime to local police, my constituent, Philip Hatch, and his son came to my office. My staff gave him a copy of the Fraud Book that this Committee produced last year and a post card that we created with tips on avoiding scams. Mr. Hatch told us that the tactics described in the materials we provided were exactly those used by the scammer. If only he had received that information sooner, he might have recognized the scam and avoided losing his hard-earned savings.

Mr. Hatch was very willing to testify today, but health issues prevent him from traveling. Instead, he graciously and courageously provided a video in order to tell his story. We will see that in a moment.

This episode demonstrates two important points. First, the criminals who prey on seniors are relentless. They will harass seniors until they have drained every penny in their life savings.

Second, this Committee's longstanding dedication to fighting fraud against seniors is raising awareness and prompting enforcement actions that are making a real difference. We must redouble our efforts to educate seniors, their families, and caregivers.

The stakes are extremely high. According to the Government Accountability Office, America's seniors lose a staggering $2.9 billion each year to an ever-growing array of financial exploitation schemes and scams.

Today's hearing coincides with the release of our Committee's 2017 Fraud Book. Like the book we published last year, it lists the top 10 scams being perpetrated against seniors, along with information on how to recognize, avoid, and report them. In both years, the IRS Impersonation Scam was the leading offender.

These lists are the result of calls made to our Committee's toll-free fraud hotline. In 2015, Hotline staff fielded more than 1,100 calls. Last year, the Hotline's call volume doubled to more than 2,200. It is clear that our efforts are raising public awareness. More important, our efforts are producing real results.

I look forward to the testimony of the Treasury Inspector General's Office today on recent evolutions in the IRS imposter scam, such as the demand for payment in iTunes gift cards, to which Mr. Hatch and many others have fallen victim. Raising awareness about the IRS scam is particularly timely, as we are now in the midst of tax filing season.

Last May, thanks to the work of our hotline investigators, TIGTA arrested five individuals in connection with the IRS imposter scam. Federal authorities believe these suspects stole almost $3 million from more than 1,200 victims. In October, 56 individuals and five call centers in India were indicted in another case.

In addition to producing criminal charges, these efforts are making it harder for criminals to find victims.

I also look forward to hearing from the Federal Trade Commission on other scams targeting seniors, such as grant scams, counterfeit check scams, and romance scams, which is timely with yesterday being Valentine's Day.

As our 2017 Fraud Book makes clear, while we are making progress, far too many victims are still losing money and, often, their retirement savings, to these criminals. Law enforcement, consumer protection, Area Agencies on Aging, and financial institutions play vital roles, but alert citizens are our first and best line of defense. I am proud of the Committee's work on this crucial issue to help seniors become more aware and informed, and to put criminals on notice that they will be stopped and brought to justice.

I now turn to Senator Casey for his opening statement.

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

Good afternoon. I am pleased to join Chairman Collins in convening this first hearing of the Special Committee on Aging for the 115th Congress. I am glad to take on the role of Ranking Member of this Committee at such a crucial time, knowing that the future of key programs for older Americans like Medicare and Medicaid are on the agenda of the new Administration. It is essential that we protect these vital programs for older Americans, and the Aging Committee has an important role to play in this work.

For today's hearing, we have the opportunity to hear from expert witnesses on the challenging issue of combatting fraud and scams targeting older Americans. Experts testifying today include Diane Menio from the Pennsylvania senior advocacy organization CARIE, a group that works every day to help older Americans live with dignity. Diane is accompanied by Charlotte Kitler, a lawyer from Nanticoke, Pennsylvania who is volunteering in her retirement years to protect her peers from fraud through her work with the Senior Medicare Patrol. I look forward to their comments as well as the testimony from our agency experts.

I'm also pleased to join with Senator Collins in releasing a Committee report detailing the top 10 scams targeting our Nation's seniors. This report is based on the experiences of more than 2,200 individuals who contacted the Committee's Fraud Hotline over the past year. What we learned from these older Americans and their families not only provided us an opportunity to help individual citizens, but it also will inform the work of this Committee going forward. And, I am pleased to have joined with Senator Collins in reintroducing the Senior$afe Act last week. This important legislation both encourages financial institutions to disclose suspected exploitation of seniors when they see it and protects them from being sued for making these reports if they have appropriately trained their staffs and make good faith reports.

In the Commonwealth of Pennsylvania, more than one-in-six residents is aged 65 or older. As a result, I know all too well how vulnerable older Americans can be to fraudsters and scam artists and other abuse. In fact, in 2015, over 22,000 cases of suspected elder abuse and neglect were reported to the Pennsylvania Department of Aging's protective services program.

That is why, last Spring, I held a field hearing of this Committee in Wilkes-Barre, Pennsylvania to hear directly from my constituents—both those affected by scams and those trying to prevent them. One constituent from Kingston Township told the heartbreaking story of scam artists attempting to steal the identify and use the credit cards of her husband of 43 years after his death. Also at the hearing, the Luzerne County District Attorney highlighted the most common type of scam happening in the county—the sweepstakes or lottery scam. This is one of the top 10 scams documented in the Committee's report and one that we will hear about from some of today's witnesses. Victims are promised lottery winnings if they just pay often sizable so-called "taxes and fees" up-front. The D.A. recalled one older victim being scammed out of $85,000 in the hopes of retrieving $1 million in fake lottery winnings.

Other common schemes include scammers impersonating IRS officials demanding payment of unpaid tax bills; those claiming to be computer support technicians to gain access to personal information stored on the computer under the guise of "fixing" it; or those claiming to be grandchildren in desperate need of a grandparents' money for bail or a hospital bill or some other emergency. While experts struggle to estimate the total financial impact of scams targeting seniors, mainly because it is so underreported, they know it adds up to nearly $3 billion a year in lost savings—and potentially billions more. It isn't just money that is lost in these scams, it is also older Americans' sense of security and financial independence. It is outrageous that people who worked hard all of their lives are being targeted for their nest-eggs when they are at their most vulnerable. And, it is wrong that seniors still feel afraid to report these schemes. They should not be embarrassed or ashamed. They should know that we have their backs and are here to help them fight back.

That is why enforcement is such a critical part of this discussion. While it may not be easy to track down these increasingly sophisticated scammers and their domestic and international networks and hold them accountable, we must do so for the safety and security of our parents and grandparents. I know that the tireless work of this Committee and the federal agencies here today has helped make progress toward this goal.

In fact, the Chair and I applauded the Federal Trade Commission and the Justice Department settlement with Western Union in which the company admitted to criminal anti-money laundering violations that have disproportionately affected aging Americans. In some instances, Western Union employees were directly respon-

sible and aided in the fraud by willfully ignoring warning signs. The $586 million settlement will be used to compensate victims of fraud where Western Union agents were complicit in the scams.

But there is more work to do, and we will continue to use the spotlight of this Committee to both help consumers understand the threat and highlight the need for action. It is for this reason that I will continue to fight to ensure that the Consumer Financial Protection Bureau has the resources to help. The CFPB houses the only federal office solely focused on sharing financial information with seniors and educating seniors about how to prevent becoming the victim of fraud. Until recently, this office was led by former Pennsylvania Secretary of Aging, Nora Dowd Eisenhower.

We also need to keep up the fight against health care fraud and abuse that we launched through the Affordable Care Act. In fact, the government has realized a record-breaking $10.7 billion in recoveries of health care fraud in the last three years. Thanks to the ACA, we have new tools like increased federal sentencing guidelines for health care fraud and enhanced screening for providers and suppliers who may pose a higher risk of fraud or abuse. And, the law provides an additional $350 million over 10 years to boost anti-fraud efforts. We also know that proposals to block grant Medicaid could present states with a significant barrier to addressing waste, fraud, and abuse in the program. Block grants could jeopardize funding for program integrity resources, as states would lose federal program integrity resources that currently go along with Medicaid matching dollars.

I look forward to hearing from our witnesses about what more we can all be doing to fight fraud and abuse.

PREPARED STATEMENT OF PHILIP HATCH

My name is Philip Hatch. I'm 81 years old, and I'm from Portland, Maine, born and raised.

I received a telephone call. I answered the phone and the man said he was a representative from the Internal Revenue Service. I said what can I do to help you? He said, "well we've gone through the records and there has been a mistake on your returns and you owe $5,988 and some odd cents." So, I said fine—tell me who I make the check out to and I'll mail it. He said "well we can't do that. We have a warrant out for your arrest. The marshals will be in your house within the hour." I said well what would you like me to do to help resolve this? They said, "you can go to CVS and get those iTunes cards and when you come back you can read the numbers off to us." I said this doesn't seem like a very professional way to do this. They said, "well it's either that or the marshals are coming. If we do this I can tell them not to come." So I did. I went and got these little iTunes cards and read them off to them and they said "alright you can't tell anybody about this." I said what do you mean I can't tell anybody about this? I'm gonna tell the guy who does my tax returns. I'm a little mad at him. He made a mistake. He said, "No. Don't do that. It will all be taken care of." This started at four in the afternoon and went on to eight o'clock at night. They called me the next day and said there was mistake. I said what do you mean a mistake? It wasn't $5,900 something dollars it was $23,000. They had someone call me on the regular phone who said he was a Portland Police Officer and that they have a local warrant out for my arrest. So I put my son on the phone and he says "who's this?" They asked who this was and he gave them a phony name and said he was an FBI agent and they said "whoops" and they hung up. That was the end of it. But I had already sent in $8,000 to these people.

Being in the military and working for the government—you know when the government calls up you say aye aye sir. What do you need? Can I help you? Okay.

Maybe if I hadn't had that background, I wouldn't have been so cooperative. But I was mad—upset that I was taken in. Just give me five minutes in a room alone with these people and I'd be happy.

All I can say is just be wary. Just be careful. When it comes to someone going after your money just say 'I'll think about it tonight and get back to you tomorrow and contact someone about it.'"

HEARING BEFORE THE
SPECIAL COMMITTEE ON AGING
UNITED STATES SENATE

Stopping Senior Scams: Developments in Financial Fraud Affecting Seniors

Testimony of
Timothy P. Camus
Deputy Inspector General for Investigations
Treasury Inspector General for Tax Administration

February 1, 2017

Washington, D.C.

TESTIMONY
OF
Timothy P. Camus
Deputy Inspector General for Investigations
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
SPECIAL COMMITTEE ON AGING
UNITED STATES SENATE

"Stopping Senior Scams: Developments in Financial Fraud Affecting Seniors"

Chairwoman Collins, Ranking Member Casey, and Members of the Committee, thank you for the opportunity to testify on the topic of financial fraud affecting seniors.

We appreciate the emphasis the committee has placed on educating our senior citizens about tax-related fraud, including schemes employed by criminals who impersonate Internal Revenue Service (IRS) employees and those who use lottery or sweepstakes swindles.

The Treasury Inspector General for Tax Administration (TIGTA) was created by Congress in 1998 and is mandated to promote integrity in America's tax system. It provides independent audit and investigative services to improve the economy, efficiency, and effectiveness of IRS operations. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate individuals and groups whose criminal activities assail the reputation and integrity of the IRS. TIGTA plays the key role of ensuring that the approximately 83,000 IRS employees[1] who collected more than $3.3 trillion in tax revenue, processed more than 244 million tax returns, and issued more than $400 billion in tax refunds during Fiscal Year (FY) 2016,[2] have done so in an effective and efficient manner while minimizing the risks of waste, fraud, and abuse.

TIGTA's Office of Investigations (OI) protects the integrity of the IRS by investigating allegations of IRS employee misconduct, external threats to IRS employees and IRS data, and other attempts to impede or otherwise interfere with the IRS's ability to collect taxes, which includes the impersonation of IRS employees. Specifically, OI investigates individuals who impersonate the IRS or its employees in

---

[1] Total IRS staffing as of January 7, 2017. Included in the total are approximately 16,200 seasonal and part-time employees.
[2] IRS, *Management's Discussion & Analysis, Fiscal Year 2016.*

order to extort money from innocent taxpayers under the guise of a non-existent IRS tax liability of some kind.

TIGTA has provided ongoing oversight and testimony on the issue of tax fraud and scams. Sweepstakes and lottery scams, e-mail and phishing scams, and investment scams are among the top ten fraud schemes used by criminals to target senior citizens.[3] Senior citizens are most likely to have a "nest egg," to own their home, and/or to have excellent credit – all of which make them attractive targets for con artists.[4] In addition, financial scams often go unreported by senior citizens or can be difficult to prosecute, so they are considered a "low-risk" crime.[5]

For the purposes of this hearing, I will highlight the two major IRS-related scams that have affected taxpayers over the past several years. Since the fall of 2013, much of OI's investigative efforts and resources have been focused on the investigation of a telephone impersonation scam in which more than 1.8 million Americans reported to us that they received unsolicited telephone calls from individuals falsely claiming to be IRS or Department of the Treasury employees. In addition, the so-called "lottery scam" has reemerged as a significant threat to tax administration.

IMPERSONATION SCAM

Since October 1, 2013, more than 10,000 individuals in the United States have reported to TIGTA that they fell victim to this scam, and more than 1.8 million people reported to us that they had received a call from individuals impersonating IRS or Department of Treasury employees. The victims are of all ages, gender, economic status, and race. No one is immune from receiving the calls. I've received one myself, and I am aware of several lawmakers who have reported that they or their relatives have received calls as well. In addition, congressional offices have also referred numerous constituent complaints about the scam to TIGTA.

Here is how the scam works: The intended victim receives an unsolicited telephone call from a live person or from an automated call dialer. The caller, using a

---

[3] *Top Ten Scams Targeting Seniors*, National Council on Aging, http://www.ncoa.org/enhance-economic-security/economic-security-Initiative/savvy-saving-seniors/top-10-scams-targeting.html (last visited Jan. 19, 2017).
[4] *Common Fraud Schemes, Fraud Target: Senior Citizens*, Federal Bureau of Investigation, http://www.fbi.gov/scams-safety/fraud/seniors (last visited Jan. 19, 2017).
[5] *Top Ten Scams Targeting Seniors*, National Council on Aging, http://www.ncoa.org/enhance-economic-security/economic-security-Initiative/savvy-saving-seniors/top-10-scams-targeting.html (last visited Jan. 19, 2017).

fake name and sometimes a fictitious IRS employee badge number, claims to be an IRS or Department of the Treasury employee. The scammers use Voice over Internet Protocol technology to hide their tracks and create false telephone numbers that show up on the victim's caller ID system; this technique is known as spoofing. For example, the scammers may make it appear as though the calls are originating from the IRS, in Washington, D.C., or elsewhere in the U.S. when, in fact, they may have originated from other locations around the globe, including India.

The callers may even know the last four digits of the victim's Social Security Number or other personal information about the victim. The impersonator claims that the intended victim owes taxes to the IRS and that, if those taxes are not paid immediately, the victim will be arrested or sued. Other threats for non-payment include the loss of a driver's or business license or deportation. The impersonators often leave "urgent" messages to return telephone calls and they often call the victim multiple times.

The victims we have interviewed say the scammers who made the threatening statements as described above demanded that the victims pay the money using prepaid debit cards, wire transfers, Western Union payments, or MoneyGram® payments. The scam has continued to evolve over time. Starting in April 2016, we noted that the victims were being told to pay the impersonators using Apple iTunes® gift cards. Between April and October 2016, between 70 and 80 percent of all payments made to the scammers were made via Apple iTunes® gift cards. In all cases, by the time the victims realized that they have been scammed, the funds were long gone.

TIGTA has made numerous arrests in connection with this scam and has a variety of investigations underway. Since October 2013, TIGTA has arrested, indicted, or prosecuted approximately 70 individuals and five call centers responsible for more than $54 million paid by the victims to IRS impersonators.

For example, on July 8, 2015, the United States Attorney's Office for the Southern District of New York announced the sentencing of Sahil Patel for his role in a massive impersonation scheme. Patel pled guilty in January 2015 to conspiracy to commit extortion, conspiracy to impersonate a Federal officer, conspiracy to commit wire fraud, and aggravated identity theft.[6]

From at least December 2011 through at least November 2013, Patel, an Indian citizen, knowingly conspired with others to commit extortion by falsely impersonating a Federal officer and demanding money under such false pretense. Victims were

---

[6] S.D. N.Y. Change of Plea Transcript filed Feb. 5, 2015; S.D. N.Y. Indict. filed Oct. 9, 2014.

contacted by telephone and told they would be arrested or otherwise charged with crimes by agents of the Federal Bureau of Investigation (FBI) or the IRS if they did not make payments to Patel and his co-conspirators.[7]

Patel was sentenced to 175 months in prison, followed by three years of supervised release. The court further entered a forfeiture judgment in the amount of $1 million against Patel.[8]

In another case, Kaushik K. Modi, also known as Kaushik K. Patel[9], a native of India who is living illegally in the United States, pled guilty on March 22, 2016 in the District of Maryland to money laundering conspiracy charges for his role in an impersonation fraud scheme. Sometime in early 2014, Modi was recruited by other Indian nationals to participate in a scheme to launder millions of dollars in fraud proceeds obtained from individual victims through a variety of schemes.

Modi was instructed via text messages to purchase large numbers of stored value cards, principally Green Dot® cards, and to forward the PIN numbers of the cards to other unidentified individuals. After forwarding the PIN numbers, Modi would receive instructions to use the cards, which had been loaded with monetary value by the coconspirators, to purchase money orders - principally MoneyGram® money orders at Walmart stores. He was further instructed to then deposit those money orders into bank accounts, either in Modi's name or in the names of third parties.

The money loaded onto the stored value cards by the coconspirators was derived from a variety of fraud schemes. Some of the money was derived from calls made by persons who impersonated IRS employees to convince innocent taxpayers that they owed taxes to the IRS and needed to send money to the coconspirators to avoid arrest and incarceration. On at least two occasions, victims of the IRS impersonation fraud deposited money directly into accounts held in Modi's name.

Between January 1, 2014 and March 24, 2015, Modi deposited into his bank accounts 241 money orders totaling more than $2 million, all in furtherance of the instructions he received from the coconspirators. Moreover, Modi frequently purchased the money orders using stored value cards that were activated by using the identification information of persons who were the victims of identity theft.[10]

---

[7] *Id.*
[8] S.D. N.Y. Crim. Docket as of Jan. 25, 2017.
[9] D. Md. Crim. Docket filed May 27, 2015.
[10] D. Md. Plea Agr. filed Mar. 22, 2016.

On May 12, 2016, Modi was sentenced to time served, approximately 13 ½ months.[11] He was later ordered to forfeit and/or pay restitution of more than $858,000[12] and could face deportation.[13]

In November 2015, this Committee made a direct referral to TIGTA involving a senior citizen located in Florida who was so frightened by the impersonators that he immediately drove to his local Walmart while remaining on the phone. During the drive, he crashed his vehicle and continued on foot to Walmart to obtain the MoneyGram® payment demanded by the impersonators. He subsequently reported his experience to the Aging Committee's fraud hotline, which contacted TIGTA. TIGTA special agents worked diligently on this referral and ultimately identified five suspects in Miami, Florida. On May 23, 2016, the five suspects were arrested for wire fraud and conspiracy to commit wire fraud.

The arrests were based on criminal complaints alleging that the defendants were involved in schemes to impersonate IRS agents and use the threat of arrest to obtain money from victims by falsely representing that the victims owed back taxes or other fees. According to the court documents, the suspects are responsible for almost $3 million in schemes that defrauded more than 1,200 victims.

One of the defendants, Arnoldo Mirabal, was sentenced on January 5, 2017. He received 24 months incarceration and was ordered to pay $97,486 in restitution.[14] Legal action is still pending related to the other defendants.

Most recently, after an exhaustive three-year joint investigation, the U.S. Department of Justice obtained an indictment on 56 individuals, some of whom are located in the United States, and five call centers located in India.[15] The investigation identified a total of approximately $272 million dollars of fraud and thousands of victims. The October indictment not only included charges related to the IRS impersonation scam, but also charged the individuals and call centers for fraud related to their impersonation of Department of Homeland Security agents and officials. This is the largest single domestic law enforcement action to date involving the IRS impersonation scam. The indictment is the result of countless hours of solid

---

[11] D. Md. Judgment filed June 3, 2016; D. Md. Crim. Docket as of Aug. 31, 2016.
[12] D. Md. Order of Restitution filed Aug. 17, 2016; D. Md. Consent Order of Forfeiture filed Aug. 17, 2016.
[13] D. Md. Plea Agreement filed Mar. 22, 2016.
[14] N.D. Tex. Judgment filed Jan. 6, 2017.
[15] S.D. Tex. Superseding Indict. filed Oct. 19, 2016.

investigative work, excellent cross-governmental collaboration, and the efforts of hundreds of TIGTA employees who have played a role in this investigation.

In addition to these investigative efforts, TIGTA has taken numerous other steps to combat this scam. Specifically, OI created a three-pronged "Advise and Disrupt Strategy." The first part of this strategy involved analyzing and using the telephone numbers victims reported to us. When an impersonation scam related telephone number was reported to us more than three times, OI special agents called it in order to confirm an impersonator was on the other end of the line. If it was a confirmed part of the scam, we identified the telephone carrier who owned the telephone number and requested that the carrier take the number down. Of the 1,120 telephone numbers we identified using this method, 1,056 (94 percent) were successfully shut down, sometimes within a week.

A second part of the strategy was to post scam-related telephone numbers on the Internet which allowed potential victims to search to determine if the call they received was a part of the scam.

The final part of the strategy was to deploy a TIGTA auto-dialer to call back the impersonators with a message ordering them to cease and desist their criminal activity, while also occupying the impersonators' time and telephone lines. The strategy resulted in over 141,000 auto-dialed calls back to the scammers.

In addition, we have developed an outstanding working relationship with the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) to combat this scam. Since the FTC also received reports of the impersonation scam, we agreed that research of its data would be very useful in linking the criminals to multiple victims. Over the past three years, we have partnered with the FTC to deliver multiple webinars, sponsored by the Veteran's Administration and AARP, to raise public awareness of identity theft and the IRS impersonation scam. We also began sharing information that was linked on the FTC website to help educate people.

As part of our efforts with the FTC and the FCC, we began working with the USTelecom Consortium and the Robo-Call Task Force to identify how technology might be used to stop the spoofed calls that were being placed by the Indian call centers. In one successful pilot program, TIGTA and the Department of Homeland Security worked with Verizon to block almost 2 million calls that had been spoofed to appear as though the calls were being made from the IRS.

The IRS has also assisted greatly in warning the public about the scam. We routinely updated the IRS as we noticed changes in the manner in which the scammers were using the IRS as a means to trick people into paying them money. In turn, the IRS updated its website and posted information on its own to warn taxpayers about the scam.

Further, we also identified the need for a robust public awareness campaign that included the print media, television media, and Public Service Announcement (PSA) videos. We recorded five PSA videos that received over 71,000 views, and we provided approximately 100 print and broadcast interviews, resulting in over 4,400 news stories in both large and small media markets, with an estimated 113 million views. In addition, we provided testimony about the scams to two congressional committees. The PSA videos can be viewed on our website at www.tigta.gov. The IRS also hosted the TIGTA PSA video on its website and created its own warning videos and messages

As the impersonation scam progressed, we also worked with the private sector companies who were caught in the middle of this massive fraud. The companies used by the impersonators to monetize the scam cooperated by using techniques to help warn consumers. For example, when a prepaid debit card is purchased, there is a fraud warning that now appears on the signature screen. Likewise, MoneyGram® has placed banners on its kiosks advising customers if they have been told to pay their taxes by MoneyGram®, it is a scam and they should not proceed with the transaction.

Since Apple iTunes® cards were being used 70 to 80 percent of the time by the impersonators as a means of cashing in on the fraud, Apple worked with TIGTA to create an audio message to help protect consumers. Apple also agreed to fund the nationwide distribution of this message at grocery and convenience stores, which resulted in more than 46 million consumers receiving this valuable message. Further, Walmart has also agreed to train its employees and post warning placards and fraud warning messages on cash envelopes.

As a result of these collaborative investigative and outreach efforts, TIGTA has seen a significant reduction in the effect of the impersonation scam on the public during the fall of 2016. For example, there has been a 93 percent reduction in identified victims regarding the scams, from 834 victims in October 2016 to 61 victims in December 2016. Moreover, we have also seen a reduction in victim losses from $4.2 million in October 2016, to $300,000 in December 2016, a reduction of 93 percent. Today, there are 92 percent fewer reported calls each week. However, it is critically important to note that sustained investigative efforts, and ongoing outreach to ensure

people do not become victims in the first place, is critical to ensure continued success in combating this scam.

LOTTERY SCAMS

While the impersonation scam was growing at an unprecedented rate, another scam, the lottery scam, also continued to target and victimize senior citizens. Although the lottery scam was not nearly the size or scope of the impersonation scam, its results were equally devastating for its victims. Its premise is simple: the scammer contacts the victim to advise the victim that he or she has won a lottery or some other prize, but before the winnings can be released, the victim is instructed to pay a non-existent Federal tax in order to receive the prize. Both the IRS impersonation scam and the lottery scam are very simple, but very effective in their use of the IRS as a means to cause confusion with their intended victims. Over the last several years, TIGTA has conducted investigations that have identified approximately 30 individuals who were responsible for defrauding victims out of millions of dollars related to the various lottery schemes.

For example, Reginald A. Lowe, Willie J. Montgomery, and Tanika Armstrong all pled guilty on October 25, 2016, in the District of Nevada, in connection with a telemarketing fraud scheme.[16]

From November 2008 to September 2013, Lowe, Montgomery, and others devised a scheme to defraud and obtain money by means of false and fraudulent pretenses. As part of the scheme, they obtained "lead sheets," which identified persons who had previously entered sweepstakes, lotteries, or other prize-drawing contests, and who were thus thought to be susceptible to misrepresentations regarding potentially winning a prize, sweepstakes, or lottery. The defendants knew these leads typically consisted of contact information for elderly or retirement-age people or others who were particularly vulnerable or susceptible to schemes.

The conspirators, in the role of "talkers," would contact potential victims by telephone and falsely represent to them that they had won prizes consisting of large amounts of cash or other high-value merchandise. In doing so, the talker would represent himself as an official or employee of a lottery/sweepstakes committee or a Government regulatory authority. The talker would frequently represent himself to be an official or employee of the IRS and would then tell the victim that in order to receive

---

[16] D. Nev. Crim. Docket as of Nov. 18, 2016.

the prize, he or she must first send money as payment for taxes on prize winnings or other fees.

In total, the conspirators fraudulently obtained approximately $1,175,670 from the scheme, which claimed at least 66 victims from 22 different states. Lowe and Montgomery both agreed to full restitution to victims of the scheme[17] and were scheduled to be sentenced on January 25, 2017; however, on January 14, 2017, Lowe passed away while in custody awaiting his sentencing hearing.[18] Montgomery's and Armstrong's sentencing hearings are scheduled for April 2017.[19]

In another case, convicted fraudsters Kenneth Kaufman and Kecia Place willfully conspired to devise a scheme to defraud and to obtain money through the use of materially false and fraudulent representations from early 2014 until February 2015. The conspirators contacted individuals and falsely advised them that they had to first pay a sum of money to cover taxes or fees in order to receive the lottery or prize money. Victims were instructed to send the taxes or fees through a variety of methods, such as a U.S. Postal Money Order, check, or direct deposit of funds into bank accounts established for the scheme, or via Western Union or MoneyGram® funds sent to the conspirators. Kaufman and Place received approximately $380,000 from at least 20 victims.[20]

Kaufman was sentenced to 33 months in prison, and Place was sentenced to one year and one day in prison. Kaufman was ordered to make restitution in the amount of $355,433. Place is jointly and severally liable for $78,864.50 of the restitution.[21]

Further, Daile Ferguson, was convicted and sentenced on October 11, 2016, in the Southern District of New York for conspiracy to commit wire fraud in connection with a lottery scheme.[22]

According to the court documents, Ferguson, who entered the United States using a Jamaican passport, was involved in a scheme to obtain money from elderly victims by informing them that they had won substantial cash prizes in an international sweepstakes lottery, but that before they could claim their prizes they had to pay fees

---

[17] D. Nev. Plea Agr. filed Oct. 25, 2016.
[18] D. Nev. Stipulation to Continue Sentencing Date filed Jan. 20, 2017.
[19] D. Nev. Crim. Docket as of Jan. 25, 2017.
[20] N.D. Ga. Indict. filed Mar. 18, 2015.
[21] N.D. Ga. Amended Judgment filed Jan. 7, 2016; N.D. Ga. Judgment filed Nov. 19, 2015.
[22] S.D. N.Y. Judgment filed Oct. 12, 2016; S.D. N.Y. Indict. filed Feb. 17, 2016.

and taxes. The victims sent hundreds of thousands of dollars in cash and checks to conspirators in the United States and in Jamaica. Ferguson received more than $430,000 from approximately 87 different individuals throughout the United States. Approximately 43 victims were over 70 years old and approximately 59 were over 60 years old. One of the victims, a resident of Connecticut, received a letter purporting to be from a "tax return officer" with the IRS. Additionally, the victim received several telephone calls from various individuals, including an individual who identified herself as an employee of the IRS and demanded that the victim make payments in order to receive the supposed winnings. As a result of the telephone calls and e-mails that the victim received from the conspirators, the victim sent approximately $20,000 through various means to numerous individuals, including Daile Ferguson.[23]

Ferguson was sentenced to 33 months in prison, followed by three years of supervised release. Ferguson was further ordered to pay more than $439,000 in restitution to the victims. He was scheduled to begin his sentence on January 17, 2017.[24]

In another case, Adrian Foster, who also entered the United States with a Jamaican passport,[25] pled guilty to conspiracy to commit wire fraud in the Southern District of New York on October 13, 2016.[26]

From at least 2009 until at least 2014, Foster and others participated in a telemarketing scheme to defraud victims, many of whom were elderly. Members of the conspiracy located in Jamaica telephoned individuals living in the United States and then telephoned these individuals and informed them they had won the lottery. The individuals were told they must pay various taxes and fees prior to receiving their winnings.

In total, Foster and his coconspirators defrauded the victims of more than $1 million during the course of the conspiracy.[27] Foster was sentenced to 15 months' incarceration and ordered to forfeit $23,940; however, additional restitution is pending.[28]

---

[23] S.D. N.Y. Crim. Compl. filed Dec. 16, 2015.
[24] S.D. N.Y. Judgment filed Oct. 12, 2016.
[25] S.D. N.Y. Crim. Compl. filed Mar. 11, 2016.
[26] S.D. N.Y. Crim. Docket as of Oct. 20, 2016.
[27] S.D. N.Y. Indict. filed June 13, 2016.
[28] S.D. N.Y. Judgment filed Jan. 13, 2017; S.D. N.Y. Consent Order of Forfeiture filed Jan. 13, 2017.

In a similar example, Davel Godfrey Young was sentenced on June 10, 2016 in the Northern District of West Virginia for conspiracy to commit wire fraud as a result of his role in an international lottery scheme.[29]

Young and coconspirator Zicko Peterkin, who both were residents and citizens of Jamaica, conspired with each other and others to fraudulently obtain money from U.S. citizens through an international lottery scam. Young and his coconspirators advised the victims that they were required to pay taxes and processing fees prior to the release of the lottery prizes.[30]

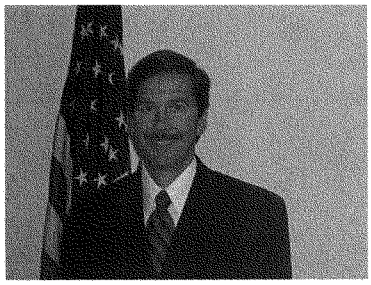
Young was sentenced to 30 months in prison. Following his prison sentence, Young will be on supervised release for 24 months and will be removed from the United States. Young was further ordered to pay more than $232,000 in restitution to victims.[31]

In summary, as can be seen by the significant investigations noted above and the resulting criminal actions taken against the defendants, we at TIGTA take seriously our mandate to protect the integrity of the IRS. As such, we plan to provide continuing investigative coverage in this area and look forward to our continued collaboration and discussions on ways we can combat these types of frauds and scams in the future.

Chairman Collins, Ranking Member Casey, and Members of the Committee, thank you for the opportunity to share my views.

---

[29] N.D. W.Va. Judgment filed June 13, 2016.
[30] N.D. W.Va. Indict. filed Sep. 4, 2013.
[31] N.D. W.Va. Judgment filed June 13, 2016.



Timothy P. Camus
Deputy Inspector General for Investigations

Mr. Timothy P. Camus has served in the Treasury Inspector General for Tax Administration (TIGTA) and the Internal Revenue Service Inspection Service, TIGTA's predecessor organization, as a Special Agent, for 25 years.

After an exemplary investigative career, Mr. Camus was promoted into TIGTA management. In June 2003, Mr. Camus became a member of the Senior Executive Service, and in January 2011 he was promoted to the position of the Deputy Inspector General for Investigations for TIGTA. As the Deputy Inspector General for Investigations, Mr. Camus is responsible for overseeing and leading all aspects of TIGTA's law enforcement mission.

During his law enforcement career, Mr. Camus has successfully investigated domestic terrorism, death threats made against public officials, bribery and extortion cases, as well as thefts of Government property and all other facets of white collar crime and fraud that impact the IRS. In 2008, Mr. Camus was awarded the Presidential Rank Award for Meritorious Service.

PREPARED STATEMENT LOIS GREISMAN

Prepared Statement of
The Federal Trade Commission

Before the
Senate Special Committee on Aging

on

Stopping Senior Scams: Developments in Financial Fraud Affecting Seniors

Washington, DC
February 1, 2017

Chairman Collins, Ranking Member Casey, and members of the Committee, I am Lois Greisman, Associate Director of the Division of Marketing Practices, in the Bureau of Consumer Protection at the Federal Trade Commission ("Commission" or "FTC").[1] I appreciate the opportunity to appear before you today to provide an overview of current trends affecting older Americans[2] and the Commission's actions to address them.

Combatting fraud is a critical component of the FTC's consumer protection mission. All consumers are potential fraud targets. While older Americans are not necessarily defrauded at higher rates than younger consumers,[3] certain types of scams are more likely to impact older Americans, such as fraudulent prize promotion schemes.[4] Such trends are crucial for the FTC to understand. According to recent U.S. Census Bureau projections, by 2030 more than 20 percent of U.S. residents will be over age 65, compared to 13 percent in 2010 and 9.8 percent in 1970.[5] As the population of older Americans grows rapidly, the FTC's efforts to identify illegal

---

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

[2] In this testimony, and in FTC enforcement cases, the terms "seniors," "older Americans," and "the elderly" refer to the population age 65 years and older, unless noted otherwise. Statistics regarding complaints to the FTC (*see* Appendix), however, use 10-year age brackets (e.g., 60-69, 70-79) because that is the manner in which age is reported in the complaints.

[3] For example, the FTC's third consumer fraud survey revealed that the overall rate of victimization for consumers age 65 and older was significantly lower than for younger consumers for the surveyed frauds. Fed. Trade Comm'n Bureau of Economics Staff Report, *Consumer Fraud in the U.S., 2011: The Third FTC Survey* ("FTC Fraud Survey"), at 56-59 (Apr. 2013), https://www.ftc.gov/reports/consumer-fraud-united-states-2011-third-ftc-survey. A fourth consumer fraud survey is in process. *See* Press Release, FTC to Conduct Consumer Fraud Survey, (Mar. 25, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-conduct-consumer-fraud-survey.

[4] *FTC Fraud Survey* at 58-59.

[5] *See* FTC Workshop, *The Changing Consumer Demographics* (Dec. 6, 2016) ("Demographics Workshop"), Jennifer Ortman, U.S. Census Bureau, Speaker Materials, Slide 23. A video of the workshop, agenda and other materials are available at https://www.ftc.gov/news-events/events-calendar/2016/12/changing-consumer-demographics; Jennifer Ortman, Victoria Velkoff, & Howard Hogan; U.S. Department of Commerce, U.S. Census Bureau, An Aging Nation: The Older Population in the United States at 1 (May 2014), https://www.census.gov/prod/2014pubs/p25-1140.pdf.

marketing impacting seniors and bring aggressive law enforcement action, as well as provide useful consumer advice, become increasingly vital.

To protect seniors, the Commission has implemented a multi-faceted approach that encompasses robust law enforcement, strategic policy initiatives, and vigorous consumer education and outreach. This testimony describes the current landscape and then outlines the Commission's various initiatives to protect older Americans.

I. Current Threats to Older Americans

Virtually every law enforcement case the Commission brings affects some seniors, and certain types of scams appear to target seniors specifically or may have a disproportionate impact on them. To identify and analyze trends regarding scams that affect different groups of consumers, the FTC assesses the marketplace in numerous ways: tracking consumer complaints; examining empirical data gathered from surveys; and investigating information from law enforcement partners and stakeholders about the issues facing consumers.

The Commission also conducts workshops and conferences to bring together law enforcement partners, industry, consumer groups, academics and others to identify new issues and collaborate on fighting fraud.[6] Since 2010, the FTC has held 33 "Common Ground" conferences around the country to engage local law enforcement officials and community organizations, including legal services providers, in the conversation about fraud. These conferences have covered a variety of consumer protection topics and looked at issues affecting a range of population segments; for example, a recent conference in Madison, Wisconsin included

[6] *See, e.g.*, FTC Workshop, *Fraud Affects Every Community* (Oct. 29, 2014), https://www.ftc.gov/news-events/eventscalendar/2014/10/fraud-affects-every-community.

a panel focused on combating fraud affecting older consumers.[7] In March, the FTC will host a workshop in partnership with the National Association of State Charities Officials, to aid in its work to combat fraud in charitable giving. This workshop will examine the demographics of those who make charitable donations, and will explore how the FTC and other consumer advocates can effectively arm consumers against charitable fundraising scams.[8]

Through these types of collaborations and our law enforcement experience, the Commission has identified several varieties of fraudulent and deceptive schemes that affect seniors[9] including: (1) sweepstakes, prize promotions, and lotteries;[10] (2) timeshare sales and re-sales;[11] (3) health care products and services;[12] (4) investments, business opportunities, and work-from-home programs;[13] (5) technical support services;[14] and (6) charitable donations.[15]

---

[7] *See* FTC Conference, *Working Together to Protect Midwest Consumers: A Common Ground Conference* (Oct. 25, 2016), https://www.ftc.gov/news-events/events-calendar/2016/10/working-together-protect-midwest-consumers-common-ground.

[8] *See* Press Release, Federal Trade Commission & National Association of State Charities Officials to Host Conference Exploring Consumer Protection Issues and Charitable Solicitations March 2017 (Nov. 15, 2016), https://www.ftc.gov/news-events/press-releases/2016/11/federal-trade-commission-national-association-state-charities.

[9] Some scams, such as Medicare imposter frauds, may be directed specifically to seniors; others, such as sweepstakes and technical support scams, may have a disproportionate impact on seniors. Many other frauds may affect seniors no more than younger consumers.

[10] *See, e.g., FTC v. Terry Somenzi*, No. 16-CV-7101 (C.D. Cal. Sept. 21, 2016), https://www.ftc.gov/enforcement/cases-proceedings/1623226/terry-somenzi-individually-officer-international-advisory (alleging defendants sent hundreds of thousands of mailings for a prize promotion scam, targeting mostly elderly consumers). *See, infra* note 44 (discussing the case as part of a coordinated effort with the Department of Justice and other entities to fight mass-mailing fraud schemes).

[11] *See, e.g., FTC v. J. William Enterprises, LLC*, No. 16-CV-2123 (M.D. Fla. Dec. 12, 2016), https://www.ftc.gov/enforcement/cases-proceedings/162-3061/j-william-enterprises-llc (alleging defendants' false promises to facilitate timeshare sales or rentals bilked $15 million from consumers).

[12] *See, e.g., FTC v. Supple, LLC*, No. 16-CV-1325 (E.D. Wis. Oct. 4, 2016), https://www.ftc.gov/enforcement/cases-proceedings/142-3231/supple-llc (alleging defendants falsely claimed supplement was scientifically proven to eliminate joint pain and completely relieved pain from arthritis and fibromyalgia); *FTC v. Mercola.com, LLC*, No. 16-CV-4282 (N.D. Ill. Apr. 13, 2016), https://www.ftc.gov/enforcement/cases-proceedings/142-3210/mercolacom-llc (alleging defendants

In addition, self-reported consumer data from our Consumer Sentinel Complaint database[16]—an online database of complaints maintained by the Commission—shows that in 2015 and 2016, consumers age 60 and older primarily complained about imposter scams, as well as telemarketing practices[17] and tech support scams.[18]

In response to these complaint trends, as well as the insights gained from our survey research and conferences, the FTC has focused its efforts to protect older consumers in three areas: (1) law enforcement targeting specific types of fraudulent and deceptive practices;

---

falsely advertised that tanning beds "reversed the appearance of aging," did not increase risk of cancer, and were approved by the FDA).

[13] *See, e.g., FTC v. Blue Saguaro Marketing, LLC*, No. 16-CV-3406 (D. Ariz. Oct. 28, 2016), https://www.ftc.gov/enforcement/cases-proceedings/162-3131-x170003/max-results-marketingblue-saguaro-marketing (charged defendants bilked seniors and veterans into buying worthless money-making opportunities and paying for phony grants program); *FTC v. Advertising Strategies, LLC*, No. 16-CV-3353 (D. Ariz. Oct. 3, 2016), https://www.ftc.gov/enforcement/cases-proceedings/162-3154/advertising-strategies-llc-et-al (charged defendants' telemarketing scheme defrauded seniors, including veterans, with bogus e-commerce money-making opportunities).

[14] *See, e.g., FTC v. Big Dog Solutions LLC*, No. 16-CV-6607 (N.D. Ill. June 24, 2016), https://www.ftc.gov/enforcement/cases-proceedings/162-3042-x160045/help-desk-national (FTC and Florida charged defendants falsely claimed that malware or hackers had compromised consumers' computers to induce purchase of tech support); *FTC v. Global Access Technical Support LLC*, No. 16-CV-1556 (E.D. Miss. Oct. 3, 2016) https://www.ftc.gov/enforcement/cases-proceedings/162-3095-x170001/global-access-technical-support (charged defendants misled consumers with pop-up ads that mimicked legitimate alerts warning consumers of computer infection).

[15] *See, e.g., FTC v. Cancer Fund of Am., Inc.*, No. 15-CV-884 (D. Ariz. Mar. 29, 2016) https://www.ftc.gov/enforcement/cases-proceedings/122-3005-x150042/cancer-fund-america-inc (FTC, all 50 states, and the District of Columbia charged that defendants claimed to help cancer patients but spent the majority of donations on their operators, families and friends, and fundraisers).

[16] In calendar year 2015, the Consumer Sentinel Network received 2,650,577 fraud and other complaints (excluding identity theft and Do-Not-Call registry complaints). Consumers reported their age in 674,000 (25%) of these complaints, with 220,965 reporting their age as 60 or older. In calendar year 2016, Consumer Sentinel received 2,651,149 fraud and other complaints. Consumers reported their age in 766,034 (29%) of these complaints, with 251,731 reporting their age as 60 or older. For information regarding the Consumer Sentinel Network, which is available to more than 2000 state, local, and federal law enforcement agencies, as well as some international partners, *see* FTC, *Consumer Sentinel Network,* https://www.ftc.gov/enforcement/consumer-sentinel-network.

[17] Complaints classified as "telemarketing practices" include an array of issues with telephone calls. However, the category does not include complaints categorized as Do-Not-Call registry complaints.

[18] *See* Appendix, Figures 1 and 2.

(2) policy initiatives designed to identify and track trends affecting older consumers; and

(3) effective education messages to help older Americans avoid common fraud schemes.

II. Law Enforcement

Aggressive law enforcement is crucial to the FTC's efforts to protect older Americans. Though all of the FTC's fraud cases involve older consumers as part of the general population, in the past three years alone the Commission has brought 25 cases alleging that defendants' conduct has specifically targeted or disproportionately harmed older adults. Many of these cases related to illegal telemarketing or deceptive marketing of health-related products and services. The FTC also has pursued actions regarding the money transfer services that are commonly used in scams affecting older adults, and has coordinated efforts with criminal and foreign law enforcement agencies to achieve a broader impact.

A. Deceptive Telemarketing

Telemarketing remains one of the most pervasive means scammers use to target consumers. It allows them to reach nearly every American consumer, wherever they may live, at minimal expense.[19] Many scammers take advantage of technological advancements in the phone system to blast millions of prerecorded messages, or robocalls,[20] to seniors. Since 2009, the Telemarketing Sales Rule has prohibited the vast majority of robocalls selling a good or service.[21] To date, the Commission has filed 45 cases against 163 companies and 121 individuals

---

[19] For example, one recent complaint alleged the defendants' cost for each robocall, on average, was a fraction of a cent. *See* Press Release, FTC Obtains Settlement Permanently Banning Vacation Package Pitchmen from Using Robocalls (Mar. 17, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-obtains-settlement-permanently-banning-vacation-package.

[20] New technologies have led to an immense source of consumer frustration – the blasting of prerecorded messages that primarily rely on Voice over Internet Protocol ("VoIP") technology. In 2016, the FTC received an average of more than 290,000 robocall complaints per month.

[21] *See* 16 C.F.R. § 310.4(b)(1)(v).

responsible for billions of illegal robocalls, as well as numerous Do-Not-Call violations. The 37 actions that have concluded have resulted in judgments totaling more than $500 million in civil penalties, redress, or disgorgement, with $29 million in collected judgments. Recently, the FTC led a multinational legal crackdown on robocallers, working with domestic and international law enforcement partners to bring nearly 40 cases against operations believed to be responsible for billions of illegal robocalls.[22] Just last month, the FTC announced actions against two massive robocall telemarketing operations, alleging that these operations together made hundreds of millions of robocalls per month.[23] The agency announced proposed settlements with many of the defendants that would permanently ban them from making robocalls.

Operations that place billions of calls to U.S. consumers affect all consumers, including seniors, but the FTC is also vigilant for evidence of schemes that specifically target the elderly. This past June, the FTC and the Florida Attorney General obtained a court order temporarily shutting down a company that allegedly bombarded consumers with illegal robocalls touting bogus credit-card interest rate reduction and debt relief services.[24] We charged that the defendants used fake company names that deceived consumers into thinking that the defendants had a relationship or affiliation with the consumers' credit-card issuers. In some instances, the

---

[22] *See* Press Release, FTC, Florida Attorney General Take Action Against Illegal Robocall Operation (June 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/ftc-florida-attorney-general-take-action-against-illegal-robocall.

[23] *See* Press Release, FTC Announces Crackdown on Two Massive Illegal Robocall Operations (Jan. 13, 2017) https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-crackdown-two-massive-illegal-robocall-operations.

[24] *See FTC v. Life Management Services of Orange County, LLC*, 6:16-CV-982-Orl (M.D. Fla. June 8, 2016), https://www.ftc.gov/enforcement/cases-proceedings/152-3216/life-management.

defendants allegedly tailored their debt elimination pitch to consumers over age 60.[25] The complaint states that this scheme bilked consumers out of more than $15.6 million since 2013.

Technical support scams also may disproportionately affect older Americans.[26] A typical technical support scam begins when a consumer receives a phone call from someone who claims, "There is a problem with your computer. I will help you fix it." The scammer then deceives the consumers into purchasing unnecessary or even harmful services to "fix" non-existent problems; consumers believe that their computer has been "fixed," but in reality it never had a problem.

In recent years, the FTC has seen a number of tech support scams employing a new twist on this model by using various methods to induce consumers to pick up the phone and place calls to the scammers. For example, last June the FTC obtained a court order temporarily shutting down an operation that allegedly used internet ads to imitate alerts on consumers' computer displays.[27] According to the FTC's complaint, the phony alerts mimicked legitimate messages from Apple or Microsoft, misleading consumers, many of whom were senior citizens, into believing their computers had serious problems and directing them to call a toll-free number.[28] Once on the phone, the operation's telemarketers allegedly claimed to "diagnose" the computer, inevitably claiming to find grave problems requiring immediate repair by a technician. The

---

[25] For example, one consumer stated that the telemarketer claimed to be offering "a program to help senior citizens eliminate their debt." *FTC v. Life Management Services of Orange County, LLC*, 6:16-CV-982-Orl, Plaintiff's Exhibit 7 (M.D. Fla. June 8, 2016).

[26] The FTC's Consumer Sentinel complaint data and law enforcement experience suggest that tech support schemes disproportionately affect older Americans.

[27] *FTC v. Big Dog Solutions LLC*, No. 16-CV-6607 (N.D. Ill. June 28, 2016), https://www.ftc.gov/system/files/documents/cases/160707helpdesknatltro.pdf; *see also* Press Release, FTC and Florida Charge Tech Support Operation with Tricking Consumers Into Paying Millions for Bogus Services, https://www.ftc.gov/news-events/press-releases/2016/07/ftc-florida-charge-tech-support-operation-tricking-consumers.

[28] *FTC v. Big Dog Solutions LLC*, No. 16-CV-6607 (N.D. Ill. June 24, 2016), https://www.ftc.gov/system/files/documents/cases/160707helpdesknatlcmpt.pdf.

scammers then allegedly charged consumers hundreds of dollars for repairs they likely did not need. Technical support scams like this one have caused consumers hundreds of millions of dollars in injury. The FTC continues to target such scammers, consulting with state and federal partners as well as researchers and computer software and manufacturing industry members, and has additional investigations underway.

Other pernicious telemarketing schemes threaten the elderly. The FTC recently brought two cases involving business opportunities that appear to have affected older adults, including veterans, looking to supplement their income.[29] In *FTC v. Advertising Strategies, LLC,* the FTC alleges that defendants told their consumer victims—many of whom are seniors or veterans—that the consumers would earn substantial income by owning or investing in e-commerce websites.[30] We contend that defendants collected hundreds or thousands of dollars from each victim, but consumers never received the promised income. In another case, the FTC charged that the defendants took money from seniors, veterans, and debt-laden consumers by selling them a worthless money-making opportunity purportedly linked to Amazon.com, and lured them with a phony grant program.[31]

In the *J. William Enterprises* case, the FTC obtained an order halting an operation in which it alleged telemarketers called timeshare owners, falsely claimed to have identified a buyer

---

[29] *FTC v. Advertising Strategies, LLC,* 2:16-cv-03353 (D. Ariz. Oct. 4, 2016), https://www.ftc.gov/enforcement/cases-proceedings/162-3154/advertising-strategies-llc-et-al; *FTC v. Blue Saguaro Marketing, LLC*, (D. Ariz. Oct. 28, 2016), https://www.ftc.gov/enforcement/cases-proceedings/162-3131-x170003/max-results-marketingblue-saguaro-marketing.

[30] Press Release, FTC Acts to Stop Telemarketing Fraud Targeting Seniors (Oct. 13, 2016), https://www.ftc.gov/news-events/press-releases/2016/10/ftc-acts-stop-telemarketing-fraud-targeting-seniors.

[31] Press Release, FTC Action Halts Telemarketing Scheme That Pitched Money-Making Opportunities and Grants (Oct. 28, 2016), https://www.ftc.gov/news-events/press-releases/2016/10/ftc-action-halts-telemarketing-scheme-pitched-money-making.

for the consumer's timeshare, and asked the consumer for a several-thousand-dollar fee.[32] Many consumers paid, but we alleged the company never delivered the promised buyers, bilking consumers out of at least $15 million. In this case, as in the other telemarketing schemes described above, many of the affected consumers were older adults.

B. Deceptive Marketing of Health-Related Products

The FTC also has focused on the deceptive marketing of health-related products promoted to older adults. Companies selling such products understandably want consumers to believe that their products will improve consumers' health or cognitive abilities. Unfortunately, unscrupulous marketers sometimes make such claims without support to substantiate their claims. The FTC actively monitors and takes action against such advertisers. For example, this past October the FTC settled an action for allegedly deceptive advertising that affected older Americans. The FTC alleged that the company, Supple, LLC, claimed its dietary supplement would completely eliminate joint pain, marketing it on television and social media touting the benefits of the product.[33] The FTC charged that, in truth, the company could not support its claims about the product, the television program was a paid infomercial, and the expert endorser, a doctor, was the CEO's wife. The company agreed to a court order requiring scientific evidence to support any future claims and imposing a $150 million judgment, most of which was suspended based on the defendants' inability to pay.

---

[32] *FTC v. J. William Enterprises, LLC*, No. 16-CV-2123 (M.D. Fla. Dec. 12, 2016), https://www.ftc.gov/enforcement/cases-proceedings/162-3061/j-william-enterprises-llc.

[33] *FTC v. Supple, LLC*, No. 16-CV-1325 (E.D. Wis. Oct. 4, 2016), https://www.ftc.gov/enforcement/cases-proceedings/142-3231/supple-llc; *see also* Press Release, Marketers of Joint Pain Supplement Agree to Settle FTC Charges of Deceptive Advertising, Endorsements (Oct. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/10/marketers-joint-pain-supplement-agree-settle-ftc-charges.

Earlier in 2016, the FTC obtained a settlement that put a stop to allegedly false and unsubstantiated marketing claims about an indoor tanning system.[34] The FTC alleged that the defendants claimed their tanning system could "reverse the appearance of aging," did not increase the risk of skin cancer, and had been endorsed by the Food and Drug Administration as safe. But, the FTC charged, the FDA had not endorsed the tanning system and there was no proof of its claimed safety or anti-aging benefits. The defendants agreed to a court order that permanently bans them from marketing or selling indoor tanning systems and requires them to issue refunds to consumers, which could cost over $5 million.

Last year, the FTC also obtained court orders as part of settlements that halted deceptive advertising about two "brain training" programs.[35] The FTC alleged that Learning RX Franchise Corp. touted its "brain training" program as clinically proven to permanently improve severe cognitive impairments such as Alzheimer's,[36] and that Lumos Labs, which created and marketed the Lumosity program, claimed that Lumosity "brain training" games could help users reduce or delay cognitive impairment associated with age and other serious health conditions.[37] The FTC charged that the companies made the claims without adequate evidence to substantiate them. The

---

[34] *FTC v. Mercola.com, LLC*, No. 16-CV-4282 (N.D. Ill. Apr. 13, 2016), https://www.ftc.gov/enforcement/cases-proceedings/142-3210/mercolacom-llc.

[35] *FTC v. LearningRx Franchise Corp.*, No. 16-CV-1159 (D. Colo. May 24, 2016), https://www.ftc.gov/enforcement/cases-proceedings/142-3206/learningrx-franchise-corp; *FTC v. Lumos Labs, Inc.*, No. 16-CV-0001 (N.D. Cal. Jan. 8, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3212/lumos-labs-inc-lumosity-mobile-online-cognitive-game.

[36] Press Release, Marketers of One-on-One 'Brain Training' Programs Settle FTC Charges That Claims about Ability to Treat Severe Cognitive Impairments Are Unsupported (May 18, 2016), https://www.ftc.gov/news-events/press-releases/2016/05/marketers-one-one-brain-training-programs-settle-ftc-charges.

[37] Press Release, Lumosity to Pay $2 Million to Settle FTC Deceptive Advertising Charges for Its "Brain Training" Program (Jan. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/01/lumosity-pay-2-million-settle-ftc-deceptive-advertising-charges.

court orders require both companies and their principals to support any health claims with clinical testing, and impose multi-million dollar judgments.

C. Money Transfer Services

Complementing these enforcement actions, the FTC has aggressively pursued the money transfer services commonly used in scams targeting older Americans. Scammers' use of these money transfer services is particularly pernicious because the victimized consumer is effectively sending cash to the scam artist, and there is no way for a consumer to get his money back once he discovers he has been deceived. Just two weeks ago, Western Union agreed to historic settlements with the FTC and the Department of Justice ("DOJ"). The FTC's action alleged that despite knowing its service was used by scammers, Western Union failed to take reasonable steps to stop the fraud.[38] For example, the FTC alleged that Western Union's own database included over 40,000 complaints about "emergency" scams, such as grandparent scams.[39] The settlement with the FTC requires Western Union to take proactive steps to prevent scammers from using its services to defraud consumers, including warning consumers about possible fraud and conducting due diligence with respect to its agents. It also calls for an independent compliance auditor to oversee Western Union's efforts for the next three years. As part of the settlements, the company has agreed to pay $586 million to redress victims.

---

[38] *FTC v. The Western Union Company*, (M.D. Penn. Jan. 19, 2017), https://www.ftc.gov/enforcement/cases-proceedings/122-3208/western-union-company.

[39] A grandparent scam involves an imposter claiming to be a grandchild in need of immediate financial help, such as money to get out of jail or to cover hospital costs. Many perpetrators in these types of cases are located overseas. *See, e.g.*, Press Release, FBI, Alleged Operator of "Grandparent Scam" Indicted (Oct. 26, 2012), http://www.fbi.gov/losangeles/press-releases/2012/alleged-operator-of-grandparent-scam-indicted.

In addition to its enforcement efforts, the FTC continues to collaborate informally with money transfer companies, reloadable prepaid card services, retailers, financial institutions, and other private sector entities to improve their fraud-prevention practices.

D. Coordinating with Criminal and Foreign Law Enforcement Agencies

The Commission has collaborated extensively with criminal and foreign law enforcement partners to combat fraud, including scams affecting the elderly. In 2003, the Commission created the Criminal Liaison Unit ("CLU") and, since that time, hundreds of fraudsters have faced criminal charges and prison time as a result of FTC prosecution referrals. For example, last year as part of a contempt action, the FTC won an award of over $17 million in sanctions against the ringleader of a prize promotion scam.[40] Through coordination with the FTC's CLU, criminal authorities recently indicted the ringleader along with a co-conspirator.[41]

The FTC, with the DOJ, also organizes and participates in the International Mass Marketing Fraud Working Group, a multilateral network of agencies that enforce laws prohibiting mass marketing fraud. The network has been pivotal in recent enforcement actions, working to dismantle a global network of mass mailing fraud schemes that allegedly defrauded millions of elderly and vulnerable consumers out of hundreds of millions of dollars. For example, in September 2016, the FTC, the DOJ, the U.S. Postal Inspection Service, the Department of the Treasury's Office of Foreign Assets Control, and a number of other domestic and foreign law enforcement partners announced civil and criminal actions against a host of

---

[40] *FTC v. Dayton Family Productions*, No. 97-CV-00750-GMN-VCF (D. Nev. Mar. 16, 2016). The decision is currently on appeal before the Ninth Circuit. The FTC's third consumer fraud survey revealed that consumers between ages 65 and 74 were more likely to be victims of fraudulent prize promotions than younger consumers. *FTC Fraud Survey*, *supra* note 3, at 59.

[41] *United States of America v. Glen Burke and Michael Rossi aka Mike Ross*, No. 2:16-cr-262 (D. Nev. Aug. 31, 2016), https://www.justice.gov/opa/file/895151/download.

defendants,[42] as well as a public education campaign.[43] As part of this effort, the FTC filed an action seeking to shut down an allegedly deceptive mail order prize promotion scheme that had mostly affected elderly consumers.[44] The FTC also provided information that led to a criminal indictment against two alleged mass-mailing fraudsters.[45]

Given the cross-border nature of many scams, the Commission also partners with multiple foreign agencies to combat fraud that affects the elderly. For example, the Commission is a member of the Centre of Operations Linked to Telemarketing Fraud ("Project COLT"), a joint operation involving U.S. and Canadian agencies to combat cross-border telemarketing fraud. Through this mechanism, the FTC coordinates law enforcement efforts and exchanges intelligence with Canadian authorities. The FTC's involvement in Project COLT has resulted in at least ten indictments of individuals involved in grandparent[46] and timeshare scams.[47] Since its inception in 1998, Project COLT has recovered more than $26 million for victims of telemarketing fraud.

---

[42] Press Release, Justice Department and Law Enforcement Partners Announce Civil and Criminal Actions to Dismantle Global Network of Mass Mailing Fraud Schemes Targeting Elderly and Vulnerable Victims (Sept. 22, 2016), https://www.justice.gov/opa/pr/justice-department-and-law-enforcement-partners-announce-civil-and-criminal-actions-dismantle.

[43] For example, the FTC has released a Mail Fraud fact sheet and a blog post to educate consumers about signs that a mailing is part of a scam. *Mail Fraud Scams*, FTC, https://www.consumer.ftc.gov/sites/default/files/ftc_pass-it-in-mail-fraud-scams_092116.pdf; Bridget Small, *Prize scams in your mailbox*, FTC (Sept. 22, 2016), https://www.consumer.ftc.gov/blog/prize-scams-your-mailbox.

[44] *See* Press Release, FTC Charges Fake Prize Scheme Operators with Fraud (Sept. 22, 2016), https://www.ftc.gov/news-events/press-releases/2016/09/ftc-charges-fake-prize-scheme-operators-fraud.

[45] *See supra* note 41.

[46] *See, e.g,* note 39, *supra.*

[47] *See, e.g.*, Press Release, FBI, Owner of Timeshare Telemarketing Fraud Sentenced to 20 Years in Prison (Jan. 29, 2014), http://www.fbi.gov/miami/press-releases/2014/owner-of-timeshare-telemarketing-fraud-sentenced-to-20-years-in-prison; Press Release, United States Attorney's Office for the Northern District of Georgia, Adams Sentenced to Over 17 Years in Prison for Multi-Million Dollar Telemarketing Fraud Scheme (Feb. 9, 2012), http://www.justice.gov/archive/usao/gan/press/2012/02-09-12.html.

Another area of international concern involves Indian call centers, which continue to be the source of various imposter frauds targeting English-speaking consumers, and appear to be responsible for many of the complaints the FTC receives from older Americans about government imposter scams and tech support scams, among other fraudulent telemarketing activity. In addition to our enforcement cases, the FTC has organized multiple stakeholder meetings, including three in India, to develop and pursue a coordinated and multi-pronged approach to this threat. The collaboration led to a four-city law enforcement training in India this past summer, in which the FTC participated, aimed at developing Indian law enforcement's capacity to arrest and prosecute the India-based individuals who perpetrate these frauds. This fall, Indian police shut down a massive telemarketing fraud ring operating outside Mumbai, arresting 70 people and questioning hundreds more.[48] The operation had allegedly targeted U.S. consumers with an IRS impersonation scam that defrauded consumers of tens of millions of dollars.[49] Shortly after the Indian police action, the DOJ unsealed an indictment charging 61 individuals with involvement in a transnational telemarketing fraud scheme operating out of a network of call centers in India and bilking U.S. consumers out of hundreds of millions of dollars

---

[48] *See, e.g.*, Shefali Anand, *Indian Police Bust IRS 'Scam Center'*, The Wall Street Journal (Oct. 5, 2016), http://www.wsj.com/articles/indian-police-detain-workers-over-possible-irs-phone-scam-1475674691.

[49] The FTC's initiative with Indian law enforcement is only one way the agency has tackled "government imposter scams"—the largest subset of complaints from older adults in Appendix, Figures 1 and 2, *infra*. For example, the FTC has brought law enforcement actions against other such scams operating domestically. *See, e.g.*, Press Release, FTC Charges Operators of Scheme that Used Fake Government Affiliation to Sell Commercial Trucking Registration Services (Oct. 17, 2016), https://www.ftc.gov/news-events/press-releases/2016/10/ftc-charges-operators-scheme-used-fake-government-affiliation; Press Release, FTC Action Halts Phony OSHA Scam that Targets New Small Businesses (June 21, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/ftc-action-halts-phony-osha-scam-targets-new-small-businesses.

using the IRS and other government imposter scams.[50] Following these actions, the number of IRS imposter scams being reported to the FTC plummeted.[51]

III. Policy Initiatives

The FTC knows it is critical to be responsive and agile in responding to challenges posed by changes in the marketplace, including rapid developments in both demographics and technology. The agency uses a variety of policy tools at its disposal to address such changes—from workshops and industry coordination to public contests seeking technological innovation.

On December 6, 2016, the Federal Trade Commission held "*The Changing Consumer Demographics*" workshop to examine the predicted population changes in the U.S. and how those changes will affect the FTC's consumer protection mission.[52] The event brought together expert demographers, marketers, consumer advocates, and law enforcement professionals to discuss how the population is shifting, how marketers are working to reach different consumer segments, and what the FTC and others can do to better reach and protect the growing population of older Americans as well as the next generation of consumers.

The population of older Americans is growing at a much faster rate than other groups. The baby boomer generation, which is driving the growth of the older population, is expected to live longer, have different expectations about retirement, and experience different economic situations than earlier generations of older adults. Panelists discussed the lack of retirement savings and the increasing need for retirees to supplement their income, as well as baby

---

[50] Press Release, Dozens of Individuals Indicted in Multimillion-Dollar Indian Call Center Scam Targeting U.S. Victims (Oct. 27, 2016), https://www.justice.gov/opa/pr/dozens-individuals-indicted-multimillion-dollar-indian-call-center-scam-targeting-us-victims.

[51] Nat Wood, *Police raids in India cut down IRS imposter calls*, FTC (Jan. 5, 2017), https://www.consumer.ftc.gov/blog/police-raids-india-cut-down-irs-imposter-calls.

[52] *See* Demographics Workshop, https://www.ftc.gov/news-events/events-calendar/2016/12/changing-consumer-demographics.

boomers' desire to travel during retirement and interest in anti-aging products.[53] Scammers often prey on the needs and desires of consumers, and the FTC will be identifying bad actors that seek to exploit the interests of aging baby boomers. The several actions the FTC has brought against telemarketers of bogus money-making opportunities and the marketers of brain-training programs and anti-aging products, mentioned earlier, reflect our ongoing vigilance in this area.

As part of its commitment to evolving to meet new challenges, the FTC also has taken steps to mount a particularized response to certain threats that exploit some recent technological changes. For example, over the past several years, FTC staff has studied extensively the problem of unwanted and illegal robocalls. This work made clear that technology would need to play a key role in ensuring consumers have the peace and protection they desire.

In response, the FTC led four public challenges to spur industry initiatives to develop solutions that will help both consumers and law enforcement combat robocalls. These challenges spurred private actors to develop consumer applications to block robocalls, as well as new law enforcement tools for use in finding and stopping robocallers.[54]

The FTC will continue to develop innovative strategies to respond to marketplace changes that will affect the next generation of aging consumers.

IV. Consumer Education and Outreach

Public outreach and education is another essential means to advance the FTC's consumer protection mission. The Commission's education and outreach programs reach tens of millions of people each year through our website, the media, and partner organizations that disseminate

---

[53] Demographics Workshop video Part 2, Panel 4, at 1:02 – 2:04.

[54] *See* https://www.ftc.gov/news-events/contests/zapping-rachel; Lesley Fair, *Robocallers find themselves in a sticky situation*, FTC (June 14, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/06/robocallers-find-themselves-sticky-situation; https://www.ftc.gov/news-events/contests/detectarobo; https://www.ftc.gov/news-events/contests/robocalls-humanity-strikes-back.

consumer information on the agency's behalf. The FTC delivers actionable, practical, plain language materials on dozens of issues, and updates its consumer education whenever it has new information to share. The Commission's library of articles in English and Spanish includes numerous pieces of particular relevance to seniors, including those specifically describing grandparent scams,[55] prize and lottery fraud,[56] medical alert scams,[57] Medicare scams,[58] technical support scams,[59] veterans' benefits scams,[60] and government imposter fraud.[61]

In addition, in 2014, the FTC created Pass It On, an innovative education effort aimed at active, older adults. Pass It On seeks to arm older people with information that they can "pass

---

[55] *See Family Emergency Scams*, FTC, https://www.consumer.ftc.gov/articles/0204-family-emergency-scams; https://www.consumer.ftc.gov/media/audio-0052-family-emergency-scams.

[56] *See Prize Scams*, FTC, https://www.consumer.ftc.gov/articles/0199-prize-scams.

[57] *See* Colleen Tressler, *To Robocall Scammers Who Lied About Free Medical Alert Devices: We've Got Your Number*, FTC (Jan. 13, 2014), https://www.consumer.ftc.gov/blog/robocall-scammers-who-lied-about-free-medical-alert-devices-weve-got-your-number; Bridget Small, *Robocall Scams Push Medical Alert Systems*, FTC (July 18, 2013), https://www.consumer.ftc.gov/blog/robocall-scams-push-medical-alert-systems.

[58] *See* Aditi Jhaveri, *Medicare imposters want to steal your money. Don't let them*, FTC (Jan. 12, 2016), https://www.consumer.ftc.gov/blog/medicare-imposters-want-steal-your-money-dont-let-them; Colleen Tressler, *Medicare 'Open Enrollment' Scams*, FTC (Nov. 5, 2015), https://www.consumer.ftc.gov/blog/medicare-open-enrollment-scams; *Medicare Fraud: Health Information for Older People*, FTC, https://www.consumer.ftc.gov/articles/0318-medicare-fraud.

[59] *See* Andrew Johnson, *Official-Sounding Calls About an Email Hack*, FTC (April 5, 2016), https://www.consumer.ftc.gov/blog/official-sounding-calls-about-email-hack; Lisa Schifferle, *FTC Cracks Down on Tech Support Scams*, FTC (Nov 19, 2014), https://www.consumer.ftc.gov/blog/ftc-cracks-down-tech-support-scams; Nicole Fleming, *Getting Your Money Back After a Tech Support Scam*, FTC (Nov. 13, 2013), https://www.consumer.ftc.gov/blog/getting-your-money-back-after-tech-support-scam; Lesley Fair, *At the Boiling Point About "Tech Support" Boiler Rooms*, FTC (Oct. 3, 2012), https://www.ftc.gov/news-events/blogs/business-blog/2012/10/boiling-point-about-tech-support-boiler-rooms; Tech Support Scams, FTC, https://www.consumer.ftc.gov/articles/0346-tech-support-scams.

[60] *See* Carol Kando-Pineda, *Veterans: Don't let scammers bilk your benefits*, FTC (Nov. 9, 2015), https://www.consumer.ftc.gov/blog/veterans-dont-let-scammers-bilk-your-benefits.

[61] *See Government Imposter Scams*, FTC, https://www.consumer.ftc.gov/articles/0048-government-imposter-scams; *Government Imposter Scams*, FTC, https://www.consumer.ftc.gov/media/audio-0053-government-imposter-scams; Amy Hebert, *Scammers Continuing to Pose as IRS Agents*, FTC (May 29, 2014), https://www.consumer.ftc.gov/blog/scammers-continuing-pose-irs-agents; Lisa Lake, *Fake IRS Collectors Are Calling*, FTC (Apr. 7, 2014), https://www.consumer.ftc.gov/blog/fake-irs-collectors-are-calling.

on" to family and friends who might need it. The materials and videos available at www.ftc.gov/PassItOn are direct and to the point, with a friendly and respectful tone informed by research about the target community's preferences. The materials cover topics such as imposter and health care scams, charity fraud, and identity theft, all of which are available in print in both English and Spanish. The Pass It On materials are in the public domain, and Committee Members or their constituents can post them, link to them, or order printed copies from www.ftc.gov/bulkorder.

In June 2016, the FTC released a new video about how an imposter scam affected a retired teacher.[62] She powerfully describes how the scam unfolded and is emphatic about helping others avoid fraud. The video is part of a video series the FTC has created to encourage people to talk about the fraud they experience. People who talk about a suspected fraud are much less likely to incur a financial loss, and they are also better able to help their friends and family avoid scams. Since June, the FTC has added videos to help consumers identify different types of imposter scams, including IRS, tech support, grandparent, and romance scams.[63] These materials are available at www.ftc.gov/PassItOnImposters. The FTC also recently unveiled a new video about the Pass It On campaign itself, and the importance of empowering older Americans to proactively pass on information to help their friends and relatives avoid being victimized.[64]

The Commission seeks to reach older adults where they gather and live: libraries, social and civic clubs, senior centers, adult living communities, and veterans' facilities. When the FTC mailed sample Pass It On information folders to three thousand such facilities, within three days

---

[62] The video is available at https://www.consumer.ftc.gov/media/video-0132-fraud-affects-every-community-medicare-scams.

[63] These videos are available at https://www.consumer.ftc.gov/media.

[64] This video is available at https://www.consumer.ftc.gov/media/video-0140-using-pass-it-your-community.

it received orders from around the country for more than two thousand copies of the materials. This confirmed the demand for clear, friendly, respectful education materials for older Americans. Indeed, since 2014, the FTC has distributed 5.9 million pieces of Pass It On print material in English and Spanish. The Commission looks forward to continuing to share these materials with public and private sector organizations.

Pass It On resources complement the FTC's other outreach and coordination activities on behalf of older people. For instance, we work extensively with the Elder Justice Coordinating Council to identify cross-agency initiatives to protect seniors from abuse, neglect, exploitation, and other crimes.[65] And, the FTC collaborated with the Consumer Financial Protection Bureau and the National Area Agencies on Aging to help produce a brochure for older adults on avoiding home improvement scams.[66]

V. Conclusion

The Commission is committed to protecting all consumers from fraud in the marketplace. To address scams that target older Americans, the agency will continue to employ a combination of law enforcement, strategic policy initiatives, and effective consumer education messages. Moreover, the Commission will continue to identify areas in which new policy and law enforcement approaches are warranted. The Commission looks forward to working with the Committee on these important issues.

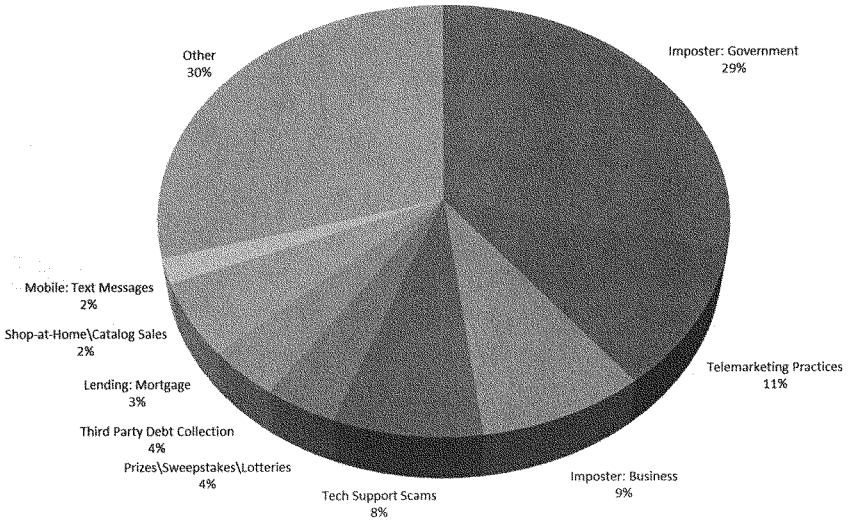
---

[65] The Secretary of the Department of Health and Human Services ("DHHS") convened the Elder Justice Coordinating Council in accordance with the Elder Justice Act of 2009. The Council consists of heads of federal departments and other government entities, including the FTC, identified as having responsibilities, or administering programs, relating to elder abuse, neglect, and exploitation. The Council's mission is to develop recommendations to the DHHS Secretary for the coordination of relevant activities. *See Facts*, Elder Justice Coordinating Council, http://ltcombudsman.org/uploads/files/issues/elder-justice-coordinating-council-factsheet.pdf (last visited January 23, 2017).

[66] *Home Improvement Scams – Tools to Reduce Your Risk*, N4A, http://www.n4a.org/Files/N4a-HI-Scams-brochure-access.pdf (last visited January 23, 2017).

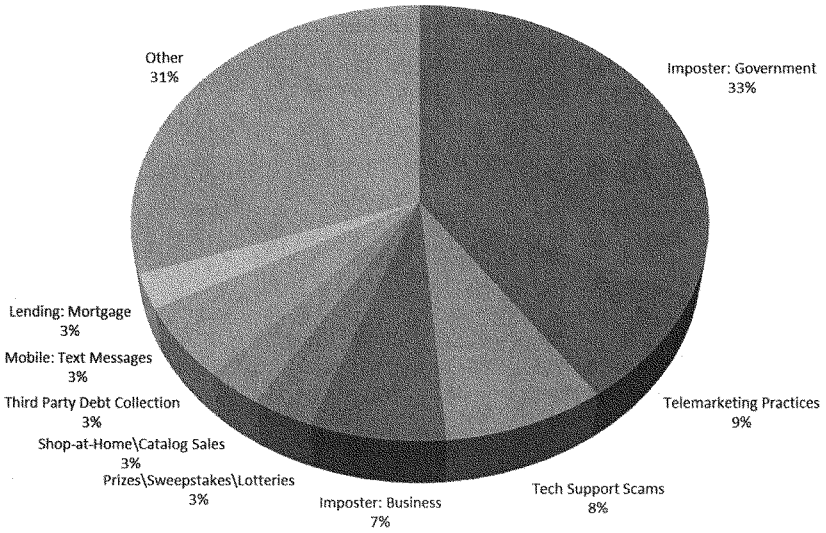
APPENDIX

Figure 1: Top Product Service Codes for Consumers Age 60 and Over in Consumer Sentinel Network Complaints January 1 - December 31, 2015[67]



[67] Percentages are based on the 220,965 complaints in 2015 where consumers reported their age as 60 and over (out of the total 674,000 who reported their age). These figures exclude Do Not Call registry and identity theft complaints. Note: The section of the chart labeled "Other" represents complaints regarding over 100 other types of products, such as counterfeit checks, credit cards, unsolicited emails, advance-fee loans and credit arrangers, and spyware\adware\malware.

Figure 2: Top Product Service Codes for Consumers Age 60 and Over in Consumer Sentinel Network Complaints January 1 – December 31, 2016[68]



[68] Percentages are based on the 251,731 complaints in 2016 where consumers reported their age as 60 and over. These figures exclude Do Not Call registry and identity theft complaints. Note: The section of the chart labeled "Other" represents complaints regarding over 100 other types of products, such as counterfeit checks, credit cards, unsolicited emails, advance-fee loans and credit arrangers, and spyware\adware\malware.

Testimony before the
US Senate Aging Committee

Wednesday, February 1, 2017

Diane A. Menio, Executive Director

Center for Advocacy for the
Rights & Interests of the Elderly
Two Penn Center ♦ 1500 John F. Kennedy Blvd. ♦ Suite 1500 ♦ Philadelphia, PA 19102
215-545-5728 ♦ 800-356-3606
menio@carie.org
www.carie.org
www.caregivergps.org

Introduction

Good morning. My name is Diane Menio and I am the executive director of the Center for Advocacy for the Rights and Interests of the Elderly (CARIE). Thank you, Senator Casey, Chairwoman Collins and members of the committee for your interest in financial exploitation, fraud and scams against the elderly and for the opportunity to present testimony today. I am pleased to be accompanied here today by Charlotte Kitler from Nanticoke, PA, a volunteer in our Pennsylvania Senior Medicare Patrol (SMP) program. In my remarks, today, I'll talk about health care fraud and abuse, scams, and financial exploitation aimed at elders.

Founded in 1977, CARIE is a nonprofit organization dedicated to improving the quality of life for vulnerable older adults. CARIE's focus of concern spans the continuum from those who live at home to those who are living in facilities. Older adults with physical or psychological impairments are often a silent group and are not able to advocate for their needs. We work to protect their rights and promote awareness of their special needs and concerns. We provide a range of services to help older victims of crime, abuse, and financial exploitation including a program that helps elder victims through the court process, assists with victim impact statements and Crime Victim's Compensation. In addition, CARIE coordinates Pennsylvania's Senior Medicare Patrol (PA-SMP) program to help fight Medicare and Medicaid fraud. We have more than 75 retired Medicare beneficiaries who provide peer education about health care fraud and share information about how to prevent becoming a victim.

Elder Abuse – the Issues

Elder abuse is a major problem that causes great suffering. Elder abuse is about 40 years behind child abuse and about 20 years behind domestic violence in terms of knowledge of the problem and a cohesive national response. The World Health Organization captured the essence of the issue when it stated, "Elder abuse is a violation of human rights and a significant cause of illness, injury, loss of productivity, isolation and despair." The mistreatment of elders occurs in both private homes and institutional settings. Elder abuse takes many forms – physical, sexual, neglect, self-neglect, psychological and financial, and it cuts across all racial, ethnic, socioeconomic, and geographic boundaries, although poverty, disability, mental incapacity, increasing old age (those 85 plus) are all factors that create the greatest risk.

According to a study published in the American Journal of Public Health, 11% of seniors interviewed reported at least one form of abuse within the past year. The report went on to say that "the rate of financial exploitation is extremely high with 1 in 20 older adults indicating some form of perceived financial mistreatment occurring at least one time in the recent past." Researchers believe that elder abuse is underreported, since many victims suffer from dementia, feel shame, or fear being forced into a nursing facility, but even so, the statistics are staggering. It is estimated that 10% of those over 60 living at home are victims of abuse and this may reflect only a fraction of the problem. Even more disturbing is that almost half of people with dementia become victims of abuse, financial exploitation, and neglect.

Financial abuse is of epidemic proportions. The MetLife Mature Market Institute estimates the annual financial loss for victims at $2.9 billion in 2010, an increase from $2.6 billion in 2008. The economic cost of elder abuse is a major drain on Medicare, Medicaid, and private dollars. Older adults depend upon these resources to help meet their needs as they age, and some lose everything including their homes. Once gone, they often never receive adequate retribution for their loss.

Medicare loses billions of dollars each year due to fraud, errors, and abuse. In 2014 testimony before this committee, the National Health Care Anti-Fraud Association placed these losses at about $60 billion annually, though the exact figure is impossible to measure. The most commonly cited range for all health care fraud estimates is 3 to 10 percent of annual health care expenditures. In 2012 Medicare expenditures were nearly $600 billion and are expected to rise as the baby boomer population ages.

The joint Department of Justice and U.S. Department of Health and Human Services (HHS) are making gains in the fight against fraud through their Medicare Fraud Strike Force. In May 2014, HHS announced that, since its inception in March 2007, Strike Force operations in nine locations have charged almost 1,900 defendants who collectively have falsely billed the Medicare program for almost $6 billion. In addition, CMS, working in conjunction with HHS-OIG, has suspended enrollments of high-risk providers in five Strike force locations and has removed more than 17,000 providers from the Medicare program since 2011

Medicare fraud, errors, and abuse can all result in higher out-of-pocket costs for beneficiaries, such as copayments for health care services that were never provided, were excessive, or were medically unnecessary. Beneficiaries may also find themselves stuck with bills for services from providers who should have billed Medicare but instead billed the beneficiary for the entire cost of that service. Finally, because Medicare numbers also contain Social Security numbers, financial fraud can be a side effect of having one's Medicare number compromised. Medicare numbers are as valuable as Social Security numbers to thieves who wish to set up credit card accounts with someone else's identity.

Unfortunately, the victimization of older adults does not end there. Various crimes, scams, schemes and frauds are routinely perpetrated on older adults often with devastating outcomes. Older adults also experience abuse and exploitation at the hands of their guardians and fiduciaries, the very people who are supposed to be responsible for their well-being.

The People who suffer

While we talk about the great toll that financial exploitation exacts on its victims, it is important to note that the problem of exploitation impacts many people whether their net worth is in the millions, the thousands or even the hundreds.

- Funeral Director Janet Powell-Dailey took advantage of three separate grieving families in their 60's, accepting money for the cremation and burial of their deceased family members. Instead, she left the three bodies in an unrefrigerated garage, where the bodies were left to decay. It was only when the odors from the rotting corpses started to seep

out of the garage that curious neighbors called the authorities and the crime was uncovered. The victims and family members who attended the preliminary hearings sat through graphic descriptions of the various state of decay of their loved ones. The defendant pleaded no contest to theft by deception and receiving stolen property. She was given a sentence of 3-23 months' house arrest, to be followed by 5 years of probation and 300 hours of community service. She will be allowed to seek employment but not in the mortuary field. She was also ordered to pay $3,482 in restitution.

- On an encouraging note, Mrs. Smith, a homebound beneficiary in central PA called us to thank us and to let us know that she received our ScamWire alert in the morning, which was included in her home delivered meal package. That same afternoon, she received a phone call from a scammer and wanted us to know that she knew not to give out any personal information because of the alert.
- We were contacted by a beneficiary who was a retired medical office worker about a company that was going around in a van, getting personal information from residents (Medicare numbers, birth dates) and dropping off scooters. When the company came to her home, she told them that she would not divulge any information, and demanded that the van driver and his counterpart leave her property immediately. After two days of harassment, she threatened to call the police and they left her alone. The company ultimately did have some information about her, and managed to bill her Medicare number for a $5,000 scooter that she never received. Several company employees and others who were involved in supplying Medicare numbers were found guilty and sentenced to prison as a result of this scam.
- A podiatrist from King of Prussia, PA billed for hundreds of services for beneficiaries she had never seen, and for people whom she had not seen in years. Some of these consumers approached our SMP staff at a presentation at a senior center attended primarily by Asian elders. They submitted Medicare Summary statements to the SMP, which were forwarded to authorities and contributed to an existing investigation by several law enforcement agencies. We later learned that she submitted fraudulent claims to Medicare totaling more than $2 million and she received at least $1.2 million in payments. Included were at least 20 claims that she had treated beneficiaries while she in fact traveling in Paris, France.
- Mary, 71, a Philadelphia resident was contacted by an individual representing himself as a spokesman for Publishers Clearing House. Mary was informed that she had won several hundred thousand dollars but had to pay the taxes on the prize. She initially sent them $200. She was contacted a second time and told that she misunderstood and needed to send an additional $2,850 in cash via USPS. Mary finally thought better of what she did and filed a police report. She initially admitted to the first mailing but at the urging of our victim advocate later attempted to make an amended report for the entire loss. (shame kept her from stating the entire loss on the first report). The police were unable to apprehend anyone at the address or telephone number that Mary provided. Nor could she get reimbursement for the money lost through Crime Victim Assistance. We have to be able to offer these victims more security.

- Sheila, 63, a Philadelphia resident was involved in an auto accident. A scammer, passing himself off as a member of the Fire Department's Special Accident Processing Unit, arrived on the scene, won her confidence and eventually scammed her out of $9,000. The case ended in a guilty plea, probation and $7,500 in restitution
- Arlene, an 80-year-old widow and resident of a continuing care community in Montgomery County, PA was overjoyed to learn that she had won $1 million, second prize, in an international lottery. The "scammers" called her on her cell phone and befriended her. They directed her how to wire moneys using Western Union and Money Gram. After almost $100,000 was wired, she then was told that the winner backed out and she was now the winner of the first-place prize, $5 million. She would need to wire larger amounts. They called her <u>every</u> day. They knew about her children and her grandchildren. She set up a new bank account transferring funds from a combined brokerage/bank account. In all she wired more than $800,000. She finally realized she was a victim after her new bank called the Pennsylvania Department of Aging and a protective services worker visited her. She had not told her family about this. The scammers told her to keep it a secret and it would be a wonderful surprise for her family. Her family eventually contacted an attorney who made complaints to the postal service, the US Attorney, the PA Attorney General without success. Arlene now has no assets beyond her monthly retirement income, she cleared out the savings that she and her husband had saved a lifetime.
- Harriet, 77, a resident of Beaver County, PA reported that she was out $2,500 after she received a call from someone posing as her "grandson" who had been arrested in Nebraska and needed the $2,500 for his release. Harriet was told to go to Walmart and send a Money Gram. Soon after the money was sent, Harriet realized she had fallen for a scam. She filed a police and an FBI report. Unfortunately, Harriet was unable to recover her funds.
- Gloria, 88 from Delaware county, PA was called by a person who claimed to be her "grandson." When she questioned why he didn't sound like himself he said that he was in an accident and the airbag hit his face. Hearing that he was in trouble, she asked how she could help him. The "grandson" said he needed money which could be delivered via ITunes gift cards. Gloria said she had never heard of ITunes gift cards. Wanting to be helpful she purchased $7,000 worth of ITunes gift cards. The "grandson" called her back and she read the numbers on the back of the cards. Thinking she was helping a loved one through a difficult time, she learned that the "grandson" she was speaking to was actually a con artist. She may have been eligible for Crime Victim's Compensation but by the time we learned of her loss, the 2-year period for recovery had expired.
- In 2012, Ray, an 89-year-old WWII veteran was befriended by a man claiming to share an interest in antique cars. Thus, began a one year deception scheme which resulted in Ray losing all of his antique cars, his home and all of his personal belongings – when we learned of his loss he was living in the only car he had left. The perpetrator carefully groomed Ray; making the him feel unsafe, threatened, and isolated. The perpetrator was arrested, tried and sentenced to 7-14 years in prison. Additionally, our colleagues at SeniorLAW Center assembled a legal team which successfully recovered his antique cars,

his belongings and reached a confidential settlement in a civil legal suit. In Ray's Own words: "I speak today for the many thousands of elderly victims as myself; in many cases the realization that you've been victimized comes too late, and the scammer has your property, and money...

Addressing the problems

The need to prevent financial exploitation is imperative. One of the solutions is for older adults and their families to talk about and plan for possible incapacity. For those showing early signs of dementia, this is particularly important, as they may eventually lose all capacity to make decisions including whom they would prefer to act on their behalf. Financial capacity is often the first type of decision-making to deteriorate with the onset of dementia or cognitive impairment, and this decline makes older adults vulnerable to abuse. Since residents of long term care facilities such as nursing homes, assisted living, personal care homes, and continuing care retirement communities may also be victimized, interventions to stop or prevent financial exploitation should also be targeted to consumers in residential settings. Based on CARIE's experience, below are the top five areas for consideration.

1. **Improving education and awareness of and intervention in financial exploitation:** More needs to be done to stress the importance of financial planning through educational campaigns targeting the general public, health care professionals, Certified Public Accountants (CPAs), and others who provide services to elders.
2. **Using fraud detection technologies:** Financial institutions should ensure that their fraud detection systems spot suspicious account activity and products associated with elder fraud risk. This includes using predictive analytics to review account holders' patterns and explore additional risk factors that may be associated with elder financial exploitation. Some signs of elder fraud risk may not match conventionally accepted patterns of suspicious activity, but nevertheless may be unusual given a particular account holder's regular behavior.
3. **Offer age-friendly services:** Banks and credit unions should enhance protections for seniors, such as encouraging them to plan for incapacity. They can offer age-friendly account features such as opt-in limits on cash withdrawals or geographic transactions, alerts for specific account activity, and offer view-only access for authorized third parties. And they can enable older consumers to provide advance consent to share account information with a trusted relative or friend when the consumer appears to be at risk.
4. **Report suspicious activity to authorities:** Financial institutions should promptly report suspected exploitation to relevant federal, state, and local authorities, regardless of whether reporting is mandatory or voluntary under state or federal law. Banks and credit unions can work closely with local Adult Protective Services and law enforcement to enhance prevention and response efforts, including expediting document requests and providing them at no charge. The Senior $afe Act Senators Casey and Collins have introduced will help advance this goal.
5. **Improve support for services, including Protective and Legal Services**: We need more workers and different types of expertise, i.e. forensic accountants to assist staff in responding to cases of financial exploitation more effectively. Every state, including Pennsylvania, has an adult protective services (APS) system authorized under state law to receive and respond to reports of abuse of elders. With more attention to elder abuse especially financial abuse many state and

local APS programs are receiving increasing numbers of reports to investigate. Unfortunately, in many jurisdictions they are being swamped as their funding has remained static and cut in many states. According to the latest data available from 2014, 34 states, use Social Services Block Grant funds to support APS, including $6.38 million in PA. This is the funding available for APS in our communities. Yet, SSBG is under major threat of elimination in the Congress. If SSBG funds were lost, states and localities would be very hard pressed to find other funding to investigate the growing numbers of abuse allegations

Other steps include encouraging law enforcement to investigate financial abuse and better publicizing victim's assistance resources.

Conclusion

Elder abuse is a problem most people would rather overlook. While we cannot alleviate all the suffering, we can do better. Fighting elder abuse requires a multidisciplinary approach but unfortunately, systems are not adequate to address all the needs. Informing the public about how to prevent elder abuse in their lives and families is a good first step. We must not let our loved ones live in isolation and we must encourage older adults and their families to talk and plan for incapacity. Older adults should be taught how to be good consumers and to reach out for help when needed. Whenever possible, we must try to better incorporate elder abuse issues into the aging, law enforcement, legal rights, mental health, and disability rights networks. We all must work to balance autonomy, privacy, and safety of older adults when confronting elder abuse.

We are pleased to see the bipartisan attention to elder fraud that the committee continues to prioritize, and that is evident in Senior $afe Act Senators Casey and Collins have introduced. We would be pleased to work along with you to help advance a positive agenda to ensure the dignity and safety of older adults. Thank you again for the opportunity to comment and for sponsoring today's hearing.

Additional Statements for the Record

601 E Street, NW | Washington, DC 20049
202-434-2277 | 1-888-OUR-AARP | 1-888-687-2277 | TTY: 1-877-434-7598
www.aarp.org | twitter: @aarp | facebook.com/aarp | youtube.com/aarp

February 6, 2017

The Honorable Susan M. Collins
United States Senate
413 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Bob Casey
United States Senate
393 Russell Senate Office Building
Washington, DC 20510

Dear Senators Collins and Casey:

On behalf of our nearly 38 million members in all 50 states and the District of Columbia, Puerto Rico, and U.S. Virgin Islands, AARP is pleased to endorse the bipartisan Senior Safe Act of 2017 (S. 223). This legislation protects individuals at financial institutions who disclose suspected financial exploitation of senior citizens to appropriate agencies, and requires the financial institution to provide training on identifying and handling of potential exploitation.

AARP has a long history of fighting for protections against the financial exploitation of older Americans and has been on the forefront of advocacy in support of federal and state laws and regulations that prevent this type of abuse. Elder abuse is an often hidden phenomenon that affects hundreds of thousands of seniors and financial exploitation is the most prevalent form of elder abuse. Every year, abuse and exploitation rob older Americans of $3 billion[1] — and this is only the amount reported.

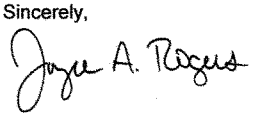
Recognizing that financial exploitation is a pervasive and increasing problem that specifically threatens our members' financial security, AARP supports strong legal protections against financial exploitation. AARP hopes this legislation is just the beginning, and we stand ready to work with you to forge solutions and bring safeguards to our members and the public.

Additional steps can be taken to include directly addressing protections on the consumer end, planning for incapacity, training for caregivers, and guidance on the common scenarios of financial exploitation. In addition, the bill can be further strengthened by including continuing education requirements and refresher training every 5 years for consumer facing individuals at financial institutions.

AARP
Alabama | Alaska | Arizona | Arkansas | California | Colorado | Connecticut | Delaware | District of Columbia | Florida | Georgia | Hawaii | Idaho | Illinois | Indiana | Iowa | Kansas | Kentucky | Louisiana | Maine | Maryland | Massachusetts | Michigan | Minnesota | Mississippi | Missouri | Montana | Nebraska | Nevada | New Hampshire | New Jersey | New Mexico | New York | North Carolina | North Dakota | Ohio | Oklahoma | Oregon | Pennsylvania | Puerto Rico | Rhode Island | South Carolina | South Dakota | Tennessee | Texas | Utah | Vermont | Virgin Islands | Virginia | Washington | West Virginia | Wisconsin | Wyoming

We look forward to working with you and your colleagues on a bipartisan basis to combat the financial exploitation of older Americans. If you have any questions, please feel free to contact me, or have your staff contact Jasmine Vasquez on our Government Affairs staff at (202) 434-3711.

Sincerely,



Joyce A. Rogers
Senior Vice President
Government Affairs

---

[i] "The Metlife Study on Elder Financial Abuse: Crimes of Occasion, Desperation, and Predation Against America's Elders" (June 2011)

January 23, 2017

Senator Susan Collins
United States Senate
Washington D.C. 20510

Senator Claire McCaskill
United States Senate
Washington D.C. 20510

Dear Senators Collins and McCaskill:

On behalf of the Conference of State Bank Supervisors (CSBS)[1], I write to express strong support for the Senior$afe Act of 2017. State regulators are committed to combatting financial abuse of elderly residents and believe that this bill recognizes the contribution of states while empowering institutions to reduce financial exploitation of the elderly.

State regulators supervise a diverse credit ecosystem, are locally-focused, and have a unique insight on the consequences of abusive practices in their communities. State banking regulators supervise over 4,500 state-chartered depository institutions, representing over 75% of our nation's banks. Additionally, most state banking departments regulate a variety of non-bank financial services providers, including mortgage lenders and consumer finance lenders.

Since the 1980s, several states have enacted laws to address the abuse, neglect, and financial exploitation of their elderly residents. These state laws provide immunity for financial service professionals to report abuse in good faith, contain penalties for failing to report or making false reports of elder abuse, and combat power of attorney abuse.[2] The Senior$afe Act of 2017 recognizes the important work of states and creates a consumer protection floor upon which states can build.

Financial services professionals are in a position of trust and have a unique window into the financial condition of seniors. Their expertise and vantage point should be leveraged to forcefully combat the growing epidemic of elder abuse.

---

[1] CSBS is the nationwide organization of banking regulators from all 50 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. For more than a century, CSBS has given state supervisors a national forum to coordinate supervision of their regulated entities and to develop regulatory policy.
[2] See: http://www.americanbar.org/groups/law_aging/resources/elder_abuse.html#banksreporting

1129 20th Street, N.W. • Ninth Floor • Washington, DC • 20036
www.csbs.org • 202-296-2840 • FAX 202-296-1928

The Senior$afe Act incentivizes financial services employees to report any suspected exploitation by making them immune from any civil or administrative liability arising from such a report, provided they exercised due care and reported in good faith. Additionally, to ensure financial services personnel have the requisite expertise, the bill requires, as a condition of receiving immunity, that financial institutions train key personnel regarding the identification and reporting of senior financial exploitation as soon as practicable.

Early detection is key to combatting elder financial abuse and to preventing abuses from occurring in the first place. Moreover, this bill can deepen the involvement of financial institutions in their community, enhance the training of financial services personnel, and reduce insured losses.

Thank you for the opportunity to share our perspective on this issue. CSBS strongly supports the Senior$afe Act and looks forward to working with you as Congress considers this legislation.

Sincerely,

John W. Ryan
President and CEO

cc:

Senator Mike Crapo
Chairman, Senate Committee on Banking, Housing, and Urban Affairs

Senator Sherrod Brown
Ranking Member, Senate Committee on Banking, Housing, and Urban Affairs

1129 20th Street, N.W. • Ninth Floor • Washington, DC • 20036
www.csbs.org • 202-296-2840 • FAX 202-296-1928

CUNA
Credit Union National Association

Jim Nussle
President & CEO

601 Pennsylvania Ave., NW
South Building, Suite 600
Washington D.C. 20004-2601

Phone: 202-508-6745
Fax: 202-638-7734
jnussle@cuna.coop

March 14, 2016

The Honorable Susan Collins
Chairman
Senate Special Committee on Aging
Washington, DC 20510

The Honorable Claire McCaskill
Ranking Member
Senate Special Committee on Aging
Washington, DC 20510

Dear Chairman Collins and Ranking Member McCaskill:

On behalf of the Credit Union National Association (CUNA), I am writing in support of S. 2216, the "Senior$afe Act of 2015." CUNA represents America's state and federally chartered credit unions and their more than 100 million members.

Financial exploitation is one of the most common forms of elder abuse. CUNA strongly supports the goal of this legislation to help seniors avoid financial exploitation and to encourage responsible decisions regarding financial management.

Many credit unions provide a full range of financial services, including financial management, retirement planning, and credit counseling to their members, including seniors and their families. Credit unions also provide elder abuse information and additional resources to help consumers, including on the credit union's websites and with account statements. The member-owner relationship between the credit union and its members puts credit union employees in a key position to detect suspicious activity around senior accounts because often times the employees know the members well. However, in some cases certain privacy laws make it difficult, or in some cases impossible, for employees to ring the alarm bell when exploitation is suspected.

S. 2216 represents an important step toward improving protection for seniors by providing legal immunity for properly trained financial services employees who disclose concerns about financial exploitation of senior citizens. As this legislation moves through the Congress, we urge you to clarify how training should be defined, and to include a more expansive description of positions defined in section 2(b)(1)(A) to include a broader scope of supervisory positions in credit unions, which may be in the position to identify senior abuse.

On behalf of America's credit unions and their more than 100 million members, thank you for your leadership on this issue.

Sincerely,

Jim Nussle
President & CEO

Free Legal Help for Maine's Seniors

December 5, 2016

Senator Susan Collins
Chair, Senate Special Committee on Aging
Dirksen Senate Office Building
Washington, DC 20510

Re: Senior$afe (S 2216)

Dear Senator Collins:

I want to thank you for inviting me to speak with the Senate Special Committee on Aging about the serious problem of financial exploitation of seniors by guardians and others in a position of power. I also want to thank you for your leadership in working to ensure there is training of financial institution employees in reporting elder abuse and an improvement in the timely reporting of financial exploitation when it is suspected through passage of the Senior$afe Act. I strongly support this legislation that is based upon work done here in Maine.

I served for over two years on the working group that developed Maine's Senior$afe training program for financial institution managers and employees. It is a voluntary training program. Through that work I came to fully appreciate the very real concerns of the financial industry regarding the consequences of violating, or being perceived as violating, the broad range of state and federal privacy laws that apply to their industry. I also came to appreciate that absent broad immunity for reporting of suspected financial exploitation, privacy regulations would continue to be a barrier to good faith reporting of suspected financial exploitation. In a landscape that includes family members who often wish to keep exploitation from coming to light because they are perpetrating the exploitation, the risk of facing potential nuisance or false complaints over privacy violations is all too real.

This is a barrier that must be removed so that financial institution employees will act immediately to make a report to the proper authorities upon forming a reasonable belief that exploitation is occurring. These professionals are on the front lines in the fight against elder financial exploitation and are often the only ones in a position to stop exploitation before it is too late.

5 Wabon Street, Augusta, Maine 04330-7040
(207) 621-0087 • Fax (207) 621-0742 • LSE Helpline 1-800-750-5353 (V/TTY: 711) • www.mainelse.org

I want to add that tying the grant of immunity to required training for not just supervisors, compliance officers, and legal advisors, but to all who come in contact with seniors as a part of their regular duties, will have the direct result of bringing more cases of exploitation to the timely attention of the proper authorities because it will significantly increase the knowledge and awareness in the industry of the red flags for elder abuse. In Maine, where our training program is entirely voluntary and carries no legal status or benefit, we have already seen what a difference training can make.

Senior$afe is a much needed step in the fight against financial exploitation of seniors and there is no doubt it will make our nation's seniors safer. I thank you again for your leadership in this important area.

Sincerely,

Jaye L. Martin
Executive Director

VIA ELECTRONIC MAIL

January 23, 2017

The Honorable Susan Collins
Chairwoman
Senate Special Committee on Aging
G31 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Robert Casey
Ranking Member
Senate Special Committee on Aging
G31 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairwoman Collins and Ranking Member Casey:

The Financial Services Institute (FSI)[1] and the 40,000 independent financial advisors and over 100 independent financial service firms that we represent strongly support the Senior$afe Act of 2017. This bill would protect certain individuals from civil or administrative liability when reporting suspected financial exploitation of an elderly person as long as the report is made "in good faith" and "with reasonable care." We believe this legislation will protect senior investors by reducing barriers for financial services professionals to report financial exploitation to state securities regulators and other appropriate governmental organizations. Therefore, we urge the Committees to support the Senior$afe Act of 2017, ensuring that financial advisors and broker-dealers have the ability to report suspicions of financial exploitation whenever they suspect fraudulent behavior without fear of liability.

FSI and its member firms are committed to the prevention elder financial abuse. Unfortunately, the victims of elder financial abuse often suffer from diminished capacity and are unable to manage their finances in line with their own self-interest and values. FSI's member firms and financial advisors commonly deal with clients who fall victim to elder financial abuse and are often the best positioned to report it. To assist our members, FSI has created an online resource center. The resource center aims to provide FSI members with helpful tools and information to identify and report elder financial abuse. In addition, FSI member firms spend considerable resources to train their financial advisors in ways to detect, prevent, and subsequently report elder financial abuse. These efforts to protect seniors will be greatly enhanced by this important legislation.

On behalf of our members, FSI appreciates your time in considering support for the Senior$afe Act of 2017. For all of the above reasons, FSI applauds both Senators Collins and McCaskill for reintroduction of the Senior$afe Act of 2017 in the 115th Congress, and we hope that the Senate will consider this worthwhile piece of legislation that will prevent the financial exploitation of seniors across the United States.

[1] The Financial Services Institute (FSI) is the only organization advocating solely on behalf of independent financial advisors and independent financial services firms. Since 2004, through advocacy, education and public awareness, FSI has successfully promoted a more responsible regulatory environment for more than 40,000 independent financial advisors, and more than 100 independent financial services firms who represent upwards of 160,000 affiliated financial advisors. We effect change through involvement in FINRA governance as well as constructive engagement in the regulatory and legislative processes, working to create a healthier regulatory environment for our members so they can provide affordable, objective advice to hard-working Main Street Americans.

If you have any questions, please contact Robert Lewis, Vice President of Legislative and Political Affairs, at (202) 803-5149.

Sincerely,

Dale E. Brown, CAE

President & CEO

cc: Members of the Senate Special Committee on Aging

Members of the Senate Committee on Banking, Housing, and Urban Affairs

Insured Retirement Institute
1100 Vermont Avenue, NW | 10th Floor
Washington, DC 20005

t | 202.469.3000
f | 202.469.3030

www.IRIonline.org
www.myIRIonline.org

January 23, 2017

Honorable Susan Collins
United States Senate
Washington, D.C. 20510

Honorable Claire McCaskill
United States Senate
Washington, D.C. 20510

Dear Senator Collins and Senator McCaskill:

On behalf of our members, the Insured Retirement Institute (IRI)[1] is pleased to once again reiterate our endorsement and strong support for expeditiously enacting the Senior$afe Act. The speedy consideration of this bill will help protect millions of older Americans who suffer financial exploitation each year, costing retirees at least $2.9 billion per year. The average loss per incident of financial exploitation is estimated to be $120,000, which is the average amount of retirement savings for an American aged 50 and older. As such, financial elder abuse can erase a lifetime of savings and leave a retiree in financial ruin.

With the population of older Americans expected to double in size to nearly 84 million Americans by 2050, this will only necessitate more concerted efforts to protect the nation's most vulnerable. Preventing financial elder abuse and protecting older Americans is at the top of IRI's legislative agenda. Our members are on the frontlines of this issue, working with clients across America every day. As a result, they are often the first to notice that a client may be the victim of a financial crime. They are all committed to protecting older Americans and ensuring that their clients' hard-earned retirement savings are protected from exploitation and fraud.

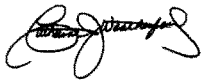
[1] The Insured Retirement Institute (IRI) is the leading association for the retirement income industry. IRI proudly leads a national consumer coalition of 40 organizations, and is the only association that represents the entire supply chain of insured retirement strategies. IRI members are the major insurers, asset managers, broker-dealers/distributors, and 150,000 financial professionals. As a not-for-profit organization, IRI provides an objective forum for communication and education, and advocates for the sustainable retirement solutions Americans need to help achieve a secure and dignified retirement. Learn more at www.irionline.org.

The Senior$afe Act will help our members and financial advisers combat financial abuse of older Americans. It would increase protections for older investors, help prevent financial exploitation, and preserve senior's hard-earned retirement savings. The legislation will foster better communications between advisors and their firms with appropriate governmental and law enforcement agencies when they suspect financial exploitation of a client. It will also encourage more firms to offer important employee training in this area.

As Congress considers legislation to increase protections from financial fraud and abuse for our seniors, allowing them to continue to enjoy a secure and dignified retirement improve retirement security, we would welcome the opportunity to work with you and your staff to advance the Senior$afe Act. Please feel free to contact me or Paul Richman, our Vice President for Government Affairs, at (202) 469-3004, if we can provide additional assistance in helping to secure passage of this vital legislation.

We thank you for your leadership in pursuing legislation that will help protect older Americans from financial exploitation.

Sincerely,



Catherine Weatherford
President & CEO
Insured Retirement Institute

cc: Honorable Mitch McConnell, Majority Leader, United States Senate
Honorable John Cornyn, Majority Whip, United States Senate
Honorable Charles Schumer, Minority Leader, United States Senate
Honorable Richard Durbin, Minority Whip, United States Senate

MAINE BANKERS
Association

January 23, 2017

Hon. Susan M. Collins
United States Senate
413 Dirksen Senate Office Building
Washington, DC 20510

RE: Senior$afe Act

Dear Senator Collins:

On behalf of the 31 member banks of the Maine Bankers Association, I thank you for re-introducing the Senior$afe Act of 2016 to the new, 115th Congress and I give you MBA's full support of your efforts. This key language clarifying the immunity provided for covered financial institutions will mean strong participation in Maine's Senior$afe program.

Maine banks working with state agencies within the Department of Professional & Financial Regulation, the Department of Health and Human Services, Legal Services for the Elderly, law enforcement and yes, the Maine Credit Union League have worked hard to bring Senior$afe to Maine's citizens. The stories where this program has saved individuals and families from financial harm are all too numerous but the common element in identifying Elder Financial Fraud is the teller or customer service representative who using Senior$afe's red flag system, spoke up and took action. Passage of your bill will mean that financial institutions will not hesitate to act due to privacy or other compliance concerns.

We appreciate your leadership on this critical issue not only for our industry but for the elderly and vulnerable citizens that will benefit by passage of this bill. Senator Collins, the Maine Bankers Association strongly supports your efforts in sponsoring the *Senior$afe Act.*

Sincerely,

Christopher W. Pinkham
President
(207) 791-8401
cpinkham@mainebankers.com

January 24, 2017

Chairman Susan M. Collins
U.S. Senate Special Committee on Aging
G31 Dirksen Senate Office Building
Washington, DC 20510

Senator Claire McCaskill
503 Hart Senate Office Building
Washington, DC 20510

Re: Senior $afe Act

Dear Chairman Collins and Senator McCaskill:

On behalf of the National Association of Insurance Commissioners (NAIC), which represents the chief insurance regulators from the 50 states, the District of Columbia, and five U.S. territories, we write to express our support for the Senior $afe Act and applaud you for your leadership to increase identification and reporting of suspected senior financial exploitation.

It is estimated that older adults in our country lose $2.9 billion annually from financial exploitation, and these losses can result in a diminished quality of life for those who fall victim to such exploitation. State insurance regulators share your commitment to protecting seniors from financial exploitation. State and federal officials entrusted with the responsibility of protecting consumers must remain vigilant in their oversight. That is why a key component of the NAIC's Retirement Security Initiative is ensuring consumers have clarity and transparency into the insurance products they are being offered, that the products are suitable for their needs, and that bad actors do not undermine efforts to address lifetime income and retirement security challenges. We look forward to continuing to work with you on these important issues.

Thank you again for your efforts to combat financial exploitation of seniors.

Sincerely,

Ted Nickel
NAIC President
Commissioner
Wisconsin Office of the
Commissioner of Insurance

Julie Mix McPeak
NAIC President-Elect
Commissioner
Tennessee Department of
Commerce & Insurance

Eric A. Cioppa
NAIC Vice President
Superintendent
Maine Bureau of Insurance

David C. Mattax
NAIC Secretary-Treasurer
Commissioner of Insurance
Texas Department of Insurance

EXECUTIVE OFFICE • 444 North Capitol Street NW, Suite 700 • Washington, DC 20001-1509 p | 202 471 3990 f | 816 460 7493
CENTRAL OFFICE • 1100 Walnut Street, Suite 1500 • Kansas City, MO 64106-2197 p | 816 842 3600 f | 816 783 8175
CAPITAL MARKETS & INVESTMENT ANALYSIS OFFICE • One New York Plaza, Suite 4210 • New York, NY 10004 p | 212 398 9000 f | 212 382 4207
www.naic.org

January 19, 2017

The Honorable Susan Collins
413 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Collins:

The National Association of Insurance and Financial Advisors (NAIFA) applauds your effort to strengthen financial protections for seniors. NAIFA supports the bipartisan, bicameral Senior$afe Act that would increase protections for senior Americans susceptible to financial and investment fraud.

For well over a century, thousands of dedicated NAIFA members have helped individuals and families reach their financial goals, and occasionally spot suspicious activities. The Senior$afe Act will remove barriers that might otherwise discourage the reporting of such suspected exploitation to authorities.

We look forward to working with you to put in place meaningful public policies to protect seniors from financial fraud and to incorporate protections for NAIFA members when reporting suspected financial abuse of a senior client. Thank you again for your leadership.

Sincerely,

Paul R. Dougherty, LUTCF, FSS, HIA
NAIFA President

2901 Telestar Ct.
Falls Church, VA
22042-1205

703-770-8100 | www.NAIFA.org

NASAA

NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION, INC.
750 First Street N.E., Suite 1140
Washington, D.C. 20002
202/737-0900
Fax: 202/783-3571
www.nasaa.org

January 24, 2017

Senator Susan Collins
Chair
U.S. Senate Special Committee on Aging
G31 Dirksen Senate Office Building
Washington, DC 20510

Re: The Senior$afe Act of 2017

Dear Senator Collins:

On behalf of the North American Securities Administrators Association ("NASAA"),[1] I am writing to express strong support for your work to better protect vulnerable adults from financial exploitation through the introduction of the Senior$afe Act of 2017. Your legislation will better protect persons aged 65 and older from financial exploitation by increasing the likelihood it will be identified by financial services professionals, and by removing barriers to reporting it, so that together we as state securities regulators and other appropriate governmental authorities can help stop it.

Senior financial exploitation is a growing problem across the country. Many in our elderly population are vulnerable due to social isolation and distance from family, caregiver, and other support networks. Indeed, evidence suggests that as many as one out of every five citizens over the age of 65 has been victimized by a financial fraud. To be successful in combating senior financial exploitation, state and federal policymakers must come together to weave a new safety net for our elderly, breaking down barriers for those who are best positioned to identify red flags early on and to encourage reporting and referrals to appropriate local, county, state, and federal agencies, including law enforcement.

The Senior$afe Act consists of several essential features. First, to promote and encourage reporting of suspected elderly financial exploitation by financial services professionals, who are positioned to identify and report "red flags" of potential exploitation, the bill would incentivize financial services employees to report any suspected exploitation by making them immune from any civil or administrative liability arising from such a report, provided that they exercised due care, and that they make these reports in good faith. Second, in order to better assure that financial services employees have the knowledge and training they require to identify "red flags" associated

[1] The oldest international organization dedicated to investor protection, the North American Securities Administrators, Inc. was organized in 1919. Its membership consists of the securities administrators in the 50 states, the District of Columbia, Canada, Mexico, Puerto Rico and the U.S. Virgin Islands. NASAA is the voice of securities agencies responsible for grass-roots investor protection and efficient capital formation.

President: Mike Rothman (Minnesota)
President-Elect: Joseph Borg (Alabama)
Past-President: Judith Shaw (Maine)
Executive Director: Joseph Brady

Secretary: Shonita Bossier (Kentucky)
Treasurer: Michael Pieciak (Vermont)

Directors: Kevin Anselm (Alaska)
Tom Cotter (Alberta)
Pamela Epting (Florida)
Melanie Senter Lubin (Maryland)

with financial exploitation, the bill would require that, as a condition of receiving immunity, financial institutions undertake to train certain personnel regarding the identification and reporting of senior financial exploitation.

The Senior$afe Act's objectives and benefits are far-reaching. Older Americans stand to benefit directly from such reporting, because early detection and reporting will minimize their financial losses from exploitation, and because improved protection of their finances ultimately helps preserve their financial independence and their personal autonomy. Financial institutions stand to benefit, as well, through preservation of their reputation, increased community recognition, increased employee satisfaction, and decreased uninsured losses.

In conclusion, state securities regulators strongly support passage of the Senior$afe Act of 2017. Please do not hesitate to contact me, or Michael Canning, NASAA Director of Policy, at (202) 737-0900, if we may be of any additional assistance.

Sincerely,

Mike Rothman
NASAA President and Minnesota Commissioner of Commerce

CC: The Honorable Claire McCaskill
United States Senator

Federal Government Affairs
600 13th Street NW
Suite 400B
Washington, DC 20005-3008

January 24, 2017

The Honorable Susan Collins
United States Senate
413 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Claire McCaskill
United States Senate
730 Hart Senate Office Building
Washington, DC 20510

Dear Senator Collins and Senator McCaskill:

Thank you for your leadership in sponsoring and for your continuing efforts to enact the Senior $afe Act. The bill will substantially aid in preventing financial exploitation of senior citizens by permitting insurance companies and agents, as well as other financial institutions, to report cases of suspected abuse to the appropriate State authorities without fear of liability. Transamerica pledges its support of your efforts to enact this important bill.

Transamerica, like most other financial services companies, has a fraud department that works to detect and properly notify the appropriate State agencies of suspected financial abuse of our senior customers. We also work to educate our distribution partners who often have the first line of contact with our policyholders regarding how to recognize financial abuse. All too often we are presented with documents or fact situations that cause us concern and warrant further investigation by the authorities. With an increasing number of seniors in our society, and as our own customers' age, we unfortunately see more and more evidence of financial abuse.

The Senior $afe Act facilitates better communication among life insurance companies, insurance producers, and regulatory agencies in the event of suspected financial exploitation of seniors.

Transamerica is the brand under which AEGON conducts business in the U.S. Transamerica is part of the AEGON group headquartered in the Netherlands, one of the world's leading life insurance and financial services organizations. The Transamerica companies market life insurance, long-term savings, pensions, accident & health, and investment products in the United States. The Transamerica companies are ranked among the top insurance groups in the U.S., based on admitted assets, and employ approximately 9600 people nationwide.

Sincerely,

Jeanne de Cervens
VP and Director, Federal Government Affairs

Part of the AEGON Group

○