S. HRG. 116–522

THAT'S NOT THE GOVERNMENT CALLING: PROTECTING SENIORS FROM THE SOCIAL SECURITY IMPERSONATION SCAM

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING

UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

WASHINGTON, DC

JANUARY 29, 2020

Serial No. 116–17

Printed for the use of the Special Committee on Aging

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

U.S. GOVERNMENT PUBLISHING OFFICE

46–704 PDF WASHINGTON : 2022

SPECIAL COMMITTEE ON AGING

SUSAN M. COLLINS, Maine, *Chairman*

TIM SCOTT, South Carolina	ROBERT P. CASEY, JR., Pennsylvania
RICHARD BURR, North Carolina	KIRSTEN E. GILLIBRAND, New York
MARTHA MCSALLY, Arizona	RICHARD BLUMENTHAL, Connecticut
MARCO RUBIO, Florida	ELIZABETH WARREN, Massachusetts
JOSH HAWLEY, Missouri	DOUG JONES, Alabama
MIKE BRAUN, Indiana	KYRSTEN SINEMA, Arizona
RICK SCOTT, Florida	JACKY ROSEN, Nevada

SARAH KHASAWINAH, *Majority Acting Staff Director*
KATHRYN MEVIS, *Minority Staff Director*

C O N T E N T S

THAT'S NOT THE GOVERNMENT CALLING: PROTECTING SENIORS FROM THE SOCIAL SECURITY IMPERSONATION SCAM

WEDNESDAY, JANUARY 29, 2020

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

The Committee met, pursuant to notice, at 9:32 a.m., in Room SD–562, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, McSally, Hawley, Braun, Casey, Gillibrand, Blumenthal, Jones, Sinema, and Rosen.

OPENING STATEMENT OF SENATOR SUSAN M. COLLINS, CHAIRMAN

The CHAIRMAN. This Committee will come to order.

Good morning. Today the Special Committee on Aging is releasing its updated 2020 Fraud Book. It lists the top 10 scams that have been reported to our Committee over the past year. The good news is that the notorious IRS Impersonation Scam, which had been the top scam reported to the Committee for 5 consecutive years, has fallen off dramatically. It used to be No. 1; now it is No. 7. Still a problem, but public awareness has certainly helped to decrease the prevalence of that scam. Unfortunately, the Social Security Impersonation Scam, the topic of this morning's hearing, has risen to take its place.

Now, reports of the SSA Scam barely registered as recently as 2017, but then it began to take off, cracking the top 10 scans reported to our Committee's Fraud Hotline in 2018 and becoming the No. 1 reported scam last year as shown on the chart displayed on the monitors.

This scam has resulted in $38 million in reported losses to Americans in 2019 alone. I suspect that that is just the tip of the iceberg because many seniors who have been affected by this scam are either too embarrassed to report their loss or do not even know who to turn to. The emotional and psychological toll for those who have lost hard-earned life savings are beyond measure.

We will hear today from Machel Andersen, who has been a victim of this ruthless scheme, and I want to personally thank Machel for her willingness to come forward and share her story, because of her willingness to do so, I am certain that there will be other older Americans who now know to just hang up the phone when they are called by somebody who is asking them for money or gift

cards and pretending to be from the Social Security Administration.

We are also very fortunate to have other terrific witnesses with us today and who are working very hard to combat this scam, and I will be introducing them at the appropriate time.

Today we will highlight the features of the Social Security Scam that are key to defeating it. Typically, the scam begins with an unsolicited robocall with a spoofed Caller ID falsely displaying the Social Security Administration as the source of the call. Now, naturally, most of us, if we see on Caller ID that the Social Security Administration is calling us, we are going to answer the phone.

The fraudster making the call will attempt to scare the victim by claiming that his or her Social Security number has been suspended due to suspicious activity, deceiving the victim so that he or she will do as instructed without question.

Now, my own 92-year-old mother received five of these Social Security Administration scam calls on her cell phone. Fortunately, she was not taken in. She knew to call me, but they were so clever and so specific, telling her that her number had been compromised, it had been used to commit fraud in Texas. There were so many details that she wisely chose to check with me to see if there could be any truth in it, but that is how clever and ruthless these criminals are. The scammer then attempts to isolate the victim so that no one can warn him or her of the scam and break the spell.

Finally, the criminals claim that the only way that the victim can resolve the problem is to provide sensitive financial information over the phone and transfer thousands of dollars to them as quickly as possible. The speed and amenity of gift cards have made them the scammers' current payment method of choice.

To emphasize the need for urgent action and the dire nature of the victim's situation, the scammers often work in teams to impersonate local law enforcement, the IRS, or other Federal officials. In one particularly outrageous case that we will hear about this morning, a criminal claimed to be the head of the Drug Enforcement Administration and even suggested to his victim that she verify his identity by looking up his name and phone number at the agency online.

To keep their victims under the spell, the scammers will demand that they cooperate with their fake investigation by the Government or face severe fines or even jail time. They also attempt to isolate the victim by keeping him or her on the phone uninterrupted for hours or even days at a time by instructing them not to tell anybody about what is going on. They will cite the confidentially of the investigation.

In a recent case reported by the Wall Street Journal, an oncology nurse in New York was instructed to leave work without notice, check into a hotel, and stay on the phone for nearly 50 hours. Coached by the fraudsters through a series of transactions at her bank and credit union, she lost almost $340,000 to scammers over 3 days.

Educating people, particularly older Americans who are more likely to be the targets, is key to defeating this scam. In today's hearing, we hope to learn more about how these fraudsters entrap their victims as well as what the Social Security Administration

has done and plans to do to get the word out to the public, to consumer groups, to businesses, and to law enforcement at every level.

We will also look at what should be done in response. In that area, I am pleased to note the late-breaking development that the Social Security Administration, working with the Office of the Inspector General and the Department of Justice, has recently filed civil suits and temporary restraining orders in two cases against five companies and three individuals. That is finally progress.

I also look forward to asking the Inspector General about new enforcement activity to stop these harmful thefts.

I appreciate all of our witnesses in joining in this effort. My hope is that our hearing today will help heighten public awareness about this scam because the best way for us to prevent this scam from ever again robbing seniors of their hard-earned savings is to prevent the scam from happening in the first place.

Thank you, and I am now pleased to turn to our 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. Thanks for holding this hearing today to discuss Social Security impersonation scams.

As everyone here knows, we are at the middle of a very important proceeding on the floor of the Senate. At the same time, for Americans who are worried about their loved ones being scammed out of their hard-earned savings, our efforts here and the efforts of others to stop con artists and fraudsters must be taken just as seriously.

It is for this reason I am pleased this Committee, the Aging Committee, is taking on this topic as the first one that we examine in the year 2020.

The Social Security impersonation scam is an imposter scam, plain and simple. In this case, however, the imposter diabolically is exploiting a public good, a benefit paid for and earned by hard working Americans, so we must not only be concerned for the sake of the individuals targeted. We also have to be concerned for the integrity of Federal departments and agencies that are tasked with serving all of us.

Just last week, as we were preparing for this hearing, one of my staff members received this message from Social Security imposters.

[Audio clip plays.]

Senator CASEY. You can tell from just that brief example how alarming this could be for someone when they are using highly charged language to get that individual's attention. Anyone—anyone—could be a victim of this kind of a crime, so one thing we have to be focused on, of course, is tracking these people down, prosecuting them and throwing them in jail, but we cannot just talk about that here. We have got to talk about ways to prevent it, and that is one of the main purposes of the hearing.

In this case, thankfully, my staff member recognized this for what it was, but not all Americans are immersed in this issue every day.

Today we are here to make clear that no one from the United States Government—no one from our Government—will ever make these types of threats.

In some ways, as Senator Collins talked about, we made some progress on the IRS version of this by warning people what the IRS would not do. We have to do the same in this case.

We need help getting this message out. Every American, particularly seniors, must be armed with information. It will take an all-hands-on-deck approach. The Committee is doing its part by releasing our 2020 Fraud Book.

When I visit senior centers in my home State of Pennsylvania, I bring copies of the report with me. Every single individual who wants a copy goes home with one. It is real bestseller at senior centers, as long as we keep bringing those copies with us.

This year, these same seniors will also be going home with a poster that inserted into the book, and that is in the back. You can take a look at that if you get a copy of it here. I want to make sure I use these visual aids.

This poster, which is not huge—but I think you get a sense of the size of it, and that gives people a lot of information that our Committee prepared.

We are grateful, Senator Collins and I are, that our staff helped us. Both staffs helped us with those, but that is another way to remind seniors. We hope that this poster will be held up by the proverbial magnets on refrigerators or other ways to remind folks about this scam.

Public awareness alone is not enough. The Federal Government has got to redouble its efforts. I know we are going to be hearing about those efforts today.

It is for this reason that I joined Senator Collins and others on the Committee in sending letters to the Social Security Administration, the Inspector General for Social Security, the Elder Justice Coordinating Committee, and the Federal Trade Commission asking for help. I know that all these entities are eager to help, to engage.

The private sector must also be involved. I have a bill with Senator Jerry Moran, the Stop Senior Scams Act, which will help banks, wire transfer companies, and retailers to train their employees to spot a scam and to stop it before money exchanges hands.

The Commerce Committee passed this bill last year without any objection. We are trying to get it through the Senate as well.

We know that con artists and scammers should not be allowed to steal money from our loved ones. Nor should they be allowed to steal our confidence in Government itself. We got a lot of work to do, and I look forward to hearing from our witnesses today and the proposals they have.

Again, I look forward to working with Chairman Collins, my colleagues on the Committee, and others in the Senate to stop these imposters in their tracks.

Thank you Chairman Collins.

The CHAIRMAN. Thank you.

I want to welcome Senator McSally and Senator Hawley to our hearing today. They have been very active members of our Com-

mittee, and we appreciate their taking the time during this very busy time for all of us.

I now want to turn to our witnesses, and I am very pleased to welcome our first panel. We have the Commissioner of the Social Security Administration, Andrew Saul. Commissioner Saul was sworn in as Commissioner in June 2019, and he immediately began taking a leadership role in the Federal response to the Social Security impersonation scam. He has a longstanding commitment to protecting and improving financial security for older Americans, having previously served for 9 years as the Chairman of the Federal Retirement Thrift Investment Board, which oversees the Federal Employee Retirement System.

Our second witness will be Gail Ennis, the Inspector General of the Social Security Administration. Inspector General Ennis was sworn in as IG in January 2019 after practicing law for more than two decades in securities litigation and banking enforcement. She has greatly increased her office's focus on the SSA scam, and we are very pleased to have two such dedicated public servants with us this morning.

Commissioner Saul, we will start with you.

STATEMENT OF HON. ANDREW SAUL, COMMISSIONER, SOCIAL SECURITY ADMINISTRATION, WASHINGTON, D.C.

Mr. SAUL. Well, thank you very much, Senators, for welcoming us here. As you said, as everybody said so far, the publicity, the education is really the most important thing, and by having this hearing, I hope we can further that goal.

Committee Chair Collins, Ranking Member Casey, and members of the Committee, I am Andrew Saul, Commissioner of the Social Security. Thank you for inviting me here today to talk about the scam crisis. Everyone here has probably received one of these scam calls, and too many people have been victimized and lost money. It is a national problem.

At first, we were not doing enough to combat these scams. That was shortsighted. The magnitude of this problem caught us off guard. Americans trust our agency and our employees, and we cannot allow swindlers to erode that trust.

In my first office visits, employees told me how these scams harm Americans and our service. We have received more and more reports from people who have been tricked by or are worried about these calls. Americans want our help on this crisis, and we also need to do critical Social Security work, like processing benefit applications and making sure we pay people the right amount.

Within a few months of getting here, I made fighting these scams and helping our front-line offices a top priority. With Inspector General Ennis' help, we started fixing things. We have been working closely with OIG, and I asked Deputy Commissioner Black to lead our efforts to curb the scams and see what more we could do. Now I believe we are on the right track. We are taking action at the national level to help front-line employees provide better service to their local communities, employees like Mr. Groshon, a district manager in Maine, who will speak to you about his office's experiences last year before we had taken on this problem.

Let me tell you about some of the things we are doing. Anyone who comes to our home page will see a bold red banner with scam information just like the one you see on the screens in this room. We are working to add messages to the pages people visit most often and here you see the—this is up from our actual web page on our home page.

We developed an online scam reporting form to help OIG get the information it needs to investigate and stop these crooks. Since this form went live in mid-November, OIG has already received over 100,000 written reports. We overhauled the OIG Fraud Hotline and improved our 800 number. Callers now hear about the scams and how to report them to OIG online. We work with OIG and major phone carriers to block calls that attempt to spoof our toll-free phone numbers from ever reaching the public.

Education is key. We are using email, television, radio, print, and social media, including YouTube, Facebook, and Twitter. Last week, we began rolling out emails to all 47 million My Social Security account holders, and we are working to add a scam awareness message to the outside of our envelopes, which will reach millions of people.

I made public service announcements that we released this month to TV and radio outlets across the country. I did an interview with AARP that focused heavily on the scams, and AARP plans to share scam information with its 38 million members.

We appreciate that Walmart work with us and OIG to display our message in over 2,000 of its stores nationwide, and we are recruiting other organizations and agencies. We have issued two recent national press releases regarding the scams, and last month, we provided every Member of Congress materials on the scam. I urge you to help us get the message out.

Everyone needs to hear this message. If a caller says there is a problem with your Social Security number or account, hang up. Do not provide them money or personal information. Report it at OIG.SSA.gov.

This is a tough problem to solve. These scams evolve as we work to shut down Social Security-related scams. Crooks likely target another agency, just as they move from IRS to Social Security Administration. Our country needs broad national solutions. We all share responsibility to fight this serious threat to the public.

If you have been tricked by these scams, you are not alone. These criminals are very good at what they do, and you should not feel embarrassed or ashamed if you are a victim. You can help protect other people by coming forward and reporting what you know to OIG.

I thank this Committee for holding this hearing to elevate the visibility of these scams and for working on solutions. I would be happy, of course, to answer any questions.

The CHAIRMAN. Thank you very much, Commissioner.

Inspector General Ennis?

STATEMENT OF HON. GAIL S. ENNIS, INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION, WASHINGTON, D.C.

Ms. ENNIS. Chairman Collins, Ranking Member Casey, and members of the Committee, thank you for inviting me to testify

about the OIG's efforts to raise public awareness and disrupt Social Security phone scams.

For the better part of a decade, Americans have been plagued by persistent robocalls and live callers who pretend to be Government employees. Too many Americans have fallen victim to these scams, believing sophisticated lies and threats, because they fear for their families, their livelihoods, or even their freedom.

We have interviewed victims, including a 30-year-old mother of two in Virginia who paid a scammer $9,000 in Target in iTunes gift cards because she had no one to care for her newborn if she went to prison, and a 75-year-old Californian who was harassed and threatened for over a month by a fake police officer. Eventually, he wired and mailed cashier's checks totaling over $260,000.

These insidious and pervasive scams have also impacted Social Security's ability to deliver its vital services timely, and they have damaged the public's trust in Social Security. To combat them, we have dedicated significant resources to investigative efforts, working with the Justice Department and other law enforcement agencies, and we have raised public awareness working with SSA and other partners to reach as many people as we can with our educational message.

I am very pleased to announce that as a result of our investigative efforts, the Department of Justice filed two civil complaints yesterday in the Eastern District of New York requesting temporary restraining orders, preliminary and permanent injunctions, and other equitable relief against five telecommunications companies and their owners.

As of this morning, one of the two temporary restraining orders covering three of the five companies and their owners has been granted, and we are hopeful the other temporary restraining order will also be granted.

According to the complaints, these companies known as "gateway carriers" facilitate the delivery of millions of fraudulent robocalls every day from foreign call centers to the United States telephone system and ultimately to the personal phones of victims throughout the United States.

These gateway carriers were notified repeatedly they were passing scam calls, yet they allowed at least hundreds of millions of scam calls into the U.S. telephone system, and they have earned a lot of money in the process in essence, profiting off of scam victims.

This civil action is the result of months of investigative work in close coordination with DOJ's Consumer Protection Branch, which heads the Transnational Elder Fraud Strike Force. The U.S. Postal Inspection Service was a partner in this effort, and other law enforcement agencies assisted, including Homeland Security's investigations, Treasury Inspector General for Tax Administration, and the Secret Service. The FTC and the FCC provided data to support the investigation.

I am particularly proud of Social Security OIG's role in the collaborative effort. Our agents and investigative counsel advocated for this top-down approach to combat the scams. We took the lead in investigating the gateway carriers, and we have played a pivotal role leading up to yesterday's filings.

We conducted a complex analysis of phone call routing, interviewed countless victims, and methodically built the Government's case.

We still have a long way to go to permanently shut down these and other gateway carriers that facilitate scam calls, and perhaps more importantly, we need to ensure we deter others from filling that void.

We continue to conduct these and other scam-related investigations. I cannot share many details, because our other investigations are ongoing, but we will update you as events unfold.

Notwithstanding all of our investigative efforts, I continue to believe that raising public awareness is the best, most effective way to combat imposter scams. No matter how many investigations we conduct or how many scammers we put out of business, there will always be more around the corner, and they will devise new ways of scamming innocent victims.

You can learn about our public outreach efforts in detail in my written statement for the record, and I will also take questions.

Despite all of our efforts, imposter scams are a broader problem than Social Security or its IG can address on our own. We need a coordinated, comprehensive approach that harnesses resources and expertise across the Federal Government for both investigative efforts and raising public awareness. Therefore, we encourage Congress to consider ways to expand upon the recently passed TRACED Act. We would like to see the law require gateway carriers to know their customers and terminate service to known scammers.

Congress could also grant asset forfeiture authority to certain agencies, allowing them to use seized funds for victim restitution or consumer protection outreach.

Thank you for holding this hearing today. Your involvement spurs increased attention to this issue and helps move us closer to a comprehensive solution. Thank you again for inviting me to testify, and I am happy to answer any questions.

The CHAIRMAN. Thank you very much.

Let me begin my comments by thanking both of you for your efforts. I will tell you that when this Committee first started becoming aware of this scam 2 years ago, we naturally contacted the Social Security Administration, the IG's office, and frankly, we had a very difficult time getting them to pay attention and realize how important it was for the agency to be front and center in communicating with beneficiaries about this scam. That has completely changed since the two of you took your positions last year.

Usually, I start my questioning by chastising the witnesses. In this case, I am going to start them by thanking both of you because you are the ones who have the access to the people who are most likely to be the victims and the means to meet them, such as through your messages to those who have online Social Security accounts, the public service messages, and the enforcement work, which I think is so important.

I want to talk a little bit about the role of these gateway telecommunications companies because in reading about the complains that were filed just yesterday, I learned that the companies that had been charged had helped to funnel some 700 million calls

through that were scam calls. That is absolutely outrageous, and they are making money from these fraudsters.

Mr. Saul, you talked about the tremendous outreach that you are doing, and, Inspector General Ennis, you talked about working on this particular case. I would like each of you to comment on what is the reaction of the telecommunication companies when you go to them and ask them to know their customers, to crack down, and to help solve this problem.

Commissioner, we will start with you.

Mr. SAUL. Well, I think that really the Inspector General has much more knowledge about this particular part of the function.

As far as I am concerned, I think that, that is a piece of the whole problem. I think the real essence and my job as Commissioner is to be sure that our beneficiaries, our customers, are aware of what a serious problem this is.

What I am trying to do and focusing the assets of our administration is on the public outreach. I mean, we are coming up with new things, actually, every week to improve the outreach that we have. We are not where we want to be yet, but we have come in the last 5 or 6 months a long, long way. I think that we were not doing the job, as I said in my statement.

This really snuck up on us. This has become a massive problem, as we all know, and it is a very serious thing. I cannot imagine an elderly person or somebody getting these calls, depending on Social Security just to buy their groceries, and they are getting threatened that, well, if they do not respond, they are not going to be getting a payment in the future.

The CHAIRMAN. Exactly.

Mr. SAUL. We have got a really big mess here. I mean, this is—and it is not going to go away quickly. I mean, I think that everything we can do—and I said this to AARP when I went over there for an interview. I said, "Whatever help you can give us, this is great." They have got 38 million members. We spent the afternoon recording a whole message of which a lot of it was dedicated to the fraud. These are things, I think, that in the end will make a really big difference.

The CHAIRMAN. I agree.

Mr. SAUL. As far as the carriers go, I would leave that to the Inspector General.

The CHAIRMAN. Absolutely.

Mr. SAUL. The outreach is what I am focusing on, Senator.

The CHAIRMAN. Inspector General Ennis, what has been the reaction of the telecom carriers?

Ms. ENNIS. The major telecom carriers have been very helpful with both us and other agencies. One of the major efforts is they help us with the Do Not Originate calls. If we can provide numbers that we know are coming, the spoofing numbers, for example, where they are spoofing Social Security numbers, if we get information to those telecoms and working with the major carriers, they can prevent up to 99 percent of those calls getting through, and so they have been a big help.

There are pockets of rural areas and other areas that are not covered by the major telecom carriers, and there are hundreds of smaller companies, and the agency has taken over the Do Not

Originate effort in contacting and reaching out to those other telecom carriers. They have sometimes more success than others. Some of the small companies do not have the technology to help us with blocking. Some of them do not want to help, but for the major carriers, as I said, we are up to 98 to 99 percent blocking, and they have been very instrumental in that.

The problem is with the gateway carriers, which frankly can operate it out of your garage. They do not need a lot of infrastructure. They do not need a lot of people. You can set up a few servers in your garage and be up and running and help transmit millions and millions and millions of calls and to introduce those calls from foreign call centers into the United States telecom system, and then they get routed around through various telecom companies. Of course, we do not work with them.

The CHAIRMAN. Good point.

Ms. ENNIS. We are working against them at this point in time and had some success yesterday, but they are the crux of the problem right now.

The CHAIRMAN. Thank you. I think that is very helpful for us to know.

One bill that I have introduced would double the penalties for people who are spoofing calls, and I think that would be helpful as well.

Senator Casey?

Senator CASEY. Thanks very much.

I want to salute the work that Inspector General Ennis and Commissioner Saul are doing on these issues as it relates especially to outreach and education as well as the effort to target those who are engaged in these kinds of scams.

Commissioner Saul, I wanted to also express my appreciation for the responsive approach you have brought to some of the work we have tried to do, in particular, reinstating regular meetings with stakeholder groups and abandoning any plans to use social media to monitor Americans with disability. I appreciate that progress.

I do have an issue I want to raise today because it is substantial and urgent. I just gave you a copy of two letters, one of which you have seen, your agency has seen yesterday. This involves continuing disability reviews.

The Social Security Administration issued a proposed rule that, in my judgment and the judgment of lots of folks around the country, would not be in the best interest of people with disabilities.

I want to quote from the letter dated yesterday. This is signed by 41 United States Senators. "The rule involves when and how often the Social Security Administration conducts these continuing disability reviews. This rule, in our judgment, would dramatically increase the number of reviews the agency conducts every year and burden millions of Americans with disabilities with more frequent and unjustified reviews of their eligibility for, one, Social Security Disability Insurance and, two, Supplemental Security Income known as the SSI benefits."

We go on to talk about our criticisms of the rule that "The administration fails to clearly establish the need for the changes to fully evaluate the effects these changes would have on bene-

ficiaries, nor does it provide an adequate cost-benefit analysis." I will not read the whole letter.

In my judgment, this rule would bury hundreds of thousands of Americans who have a disability with more administrative paperwork and also cost the agency almost $2 billion at a time when I hope there would be more effort made—and I know we have talked a bit about this—more effort made to reduce wait times and also to reduce the hearing backlog.

We know that in 2017, an estimated 10,000 people died waiting for SSDI benefits, and I know you are aware of that challenge.

I mentioned the two letters. This is noteworthy. 120,000 as of today—the comment period ends the 31st, just 2 days from now, but 120,000 Americans have submitted comments to the rule as of this morning.

I know you cannot comment directly on the rule because of the process, but I would hope—I would hope you would not continue to pursue the promulgation of this rule, and before all my time runs out, I want to make sure I just put two questions on the record. Number one, I have an additional letter that you now have. I know you will take a close look at it, but it is a long letter. It also has 37 very specific, separate criticisms of the rule. I would ask you, No. 1, to make a commitment to provide a detailed written response to me with regard to that letter. The second question I have is, Would you meet with me personally so that we can talk about this rule and the impact it can have?

I await your answer on both questions.

Mr. SAUL. Of course, the answer is yes to both of those. I am glad to meet with you, which we have met before, Senator, and I stand ready to meet with you and explain our position on these.

I just would like to say for the record, to answering, we will, of course, address this package that you have given me in a timely fashion.

Let me just say nobody here, including myself obviously, is happy with the way the disability process has worked over the years. You are absolutely right. We have had people waiting—it is a disgrace—years in some cases to get hearings. The system was completely deluged in the severe economic downturn that we had in 2008, 2009. We are recovering from it now, and if you look at our wait time for hearings now, it has dropped further than a half of where it was at its worst.

I am not happy with this, and one of the things I want to do is fix the disability process, Senator, so the next time, inevitably, unfortunately because of the economic cycles, we are going to find ourselves, hopefully, not like it was in 08 or 09, but we are going to have a downturn, and we are going to have more claims coming in, and we are going to have more hearings and everything that put us in the mess we are in.

We are doing two basic things. I do not want to take the time up here, but just to give you a little overview, the first thing we have done is we have asked Johns Hopkins Applied Physics Department, who does a tremendous amount of work for the Departments of Defense and Navy on health care, disability, just very similar to what we have, to come in and to study our whole disability process from beginning to end. They are in the midst of

their survey. This is not a big expensive consultant thing but very limited, with a very few very bright people from Hopkins that understand this, and we are in the midst of their work. I believe we will have a report within the next 2 weeks, and from what I have heard, they are going to have major recommendations to fix the way the work flows and the processes work in the disability operation.

Senator CASEY. We are out of time, but I just——

Mr. SAUL. Right. That is one.

Senator CASEY. Okay.

Mr. SAUL. Just let me say the second thing, as far as the regulations go, we have regulations that have not been updated for 50 years, Senator. The workforce has changed completely. Obviously, thank God, health care has changed completely. I feel it is my responsibility to bring these regulations and the disability procedures up to date, and that is why I feel so strongly about the regulations. I am glad to sit down with you at any time at your convenience.

Senator CASEY. Thank you.

Chairman Collins?

The CHAIRMAN. Senator Casey raises a very important issue, and I am glad you are going to meet. I do hope we can get back to the topic of this hearing, and I would like to call next on Senator McSally.

Senator MCSALLY. Thank you, Chairwoman Collins and Ranking Member Casey, for holding this really important hearing.

As was already discussed yesterday, we learned the Justice Department has sought restraining orders against two companies, one of which is in Arizona, my State. That facilitated hundreds of millions of fraudulent robocalls coming into the U.S. from overseas. TollFreeDeals.com in Arizona carried 720 million calls in just a 23-day period, most of which lasted for less than a second.

Going after these companies is a first-of-a-kind action, and I really applaud all the effort it took to get to this place.

As was also mentioned in this Wall Street Journal article, it talks about the challenges that both these companies operate out of residential addresses, with little more than a server and other basic equipment.

I have said this in this Committee before. There is a special place in hell for people who are scamming our veterans—I have said that before—and our seniors and figuring out how to profit off taking away their life savings in this way. I am disgusted that there is an Arizonan who is doing this.

I want to applaud the efforts. How do we even find these if people can operate with a server out of their garage? Maybe you do not want to tip your hand as to how we do that, but can you share a little bit more, Ms. Ennis, about the challenges of even getting to identify these awful companies that are preying upon our seniors, and what more can be done?

Ms. ENNIS. The challenges are great, and it takes a lot of just hard work from our investigative team. We have had agents working on this for quite some time. It is a lot of analysis, a lot of tracking things down.

The new online form that the agency helps us develop has been instrumental in helping us move this case along a little bit better

because we get more real-time information. Prior to our getting real-time information from the online reporting, we had processing time, and things took days to get to us. Real-time information is critical because these are fast-moving cases because once someone transmits their money to the money mules who move the money around, if you cannot track that money mule, you have lost the money. You have lost the trail, so it really has just been many, many hours of dedicated work from our investigators to talk to victims, to look at phone patterns, and to look at the data that we are collecting to do this.

What more we can do is just—because we are a small agency as compared to some other law enforcement—I have 550, give or take, total employees. Only several hundred are in the investigative side, and so what we have done is try to amplify our forces by joining forces with other Federal law enforcement and State and local partners, which does give us a broader footprint around the country. We have also developed a major case unit within the OIG, so that we can coordinate these efforts better and work better with our law enforcement partners.

We are doing what we can being a small force but a mighty force and working with other Federal law enforcement to help us.

Senator MCSALLY. Great. Thank you.

A constituent of mine named Charles McNally—not related, different spelling, McNally of Tucson—called the Senate Aging Fraud Hotline and alerted that he had been approached by what he believed to be a Social Security scam. Thankfully, once the scammers instructed him to buy and send gift cards, he became suspicious, cutoff communication, and he told us about the story. Unfortunately, Charles had already given the scammer his Social Security number.

In addition to seniors giving up their hard-earned life savings, giving up their Social Security number can obviously leave them susceptible to identity theft and other ways to rob them.

Do you also, either of you, have any perspective on sharing how we are getting to the root issues of maybe someone realizes it as they are moving down this road, like Charles, but he already gave up his Social Security number?

Ms. ENNIS. Right. The problem with identity theft is enormous, and even though they are looking to steal money, they can also be stealing and then selling identity information.

It is a little harder to understand whether then that information that may be used came from this scam or something else——

Senator MCSALLY. Right, right.

Ms. ENNIS [continuing]. because, unfortunately, there are so many ways today that thieves can acquire your personal information, through phishing, email scams, through other identity theft operations, and then they sell it on the dark web.

We are learning a lot more as we investigate, and I can assure you that as we investigate these cases, if there are things that we can do to try to help prevent further use of personal information that may have been acquired, we will do everything we can to stop it.

In the meantime, we advise anyone to go to the FTC's website where they give information to consumers and people about what

to do if you believe your identity has been stolen and how to best protect yourself against that.

Senator MCSALLY. Wonderful. Thank you.

I really want to applaud the outreach efforts that you are making, Commissioner Saul. My mom and many of my constituents who are seniors are probably not up on Twitter and YouTube, so these other more traditional ways to communicate to them are really important.

I am up on your Social Security system. I am like a secret shopper to see what emails are being sent out. I just actually looked it up. I had a couple emails this year about reviewing my accounts or anything. Maybe they went to spam, but I have not seen anything specifically related to alerts on scams.

I think pushing out via email—many seniors like my mom and those in Arizona, they will be up on email if they are not up on other, and then traditional through the mail as well. I would just encourage you to keep it going—the more information the better—to help with the education.

I know I am over my time, but do you have any other comments on that?

Mr. SAUL. Just to tell you that this is a continuing effort. We appreciate your support. You can be assured that we are just beginning this quest. I mean, we are into this. I promise you.

Senator MCSALLY. Wonderful. Thank you.

Thank you, Madam Chairman.

The CHAIRMAN. Thank you very much.

Senator Hawley?

Senator HAWLEY. Thank you, Madam Chair. Thank you for hosting, for calling this hearing today.

Commissioner, let me start with you. I am struck by the fact that these reports of scams with the SSA has displaced what was the most popular, most prevalent scam in recent years, which is IRS scamming. On that note, I am just wondering, have you consulted with officials, you or your administration consulted with officials at the IRS to see what worked or did not work for them in combating that very prevalent IRS scam in recent years?

Mr. SAUL. Well, I guess we are the lucky ones now, Senator. They have shifted to us, and as I said, I do believe that this is going to be expanded unless we can really do a good job in cutting it off.

Yes. Our people obviously have talked to, looked at other agencies—Justice Department. The Inspector General, of course, is working with other agencies, and so is our people. A lot of the efforts that we are doing—various mailers, social media—all these efforts, a lot of it is based on learning from other agencies.

Senator HAWLEY. Are there lessons in particular that stand out from the agencies that you have consulted with, whether it is the IRS, DOJ, or others?

Mr. SAUL. I am not sure of that. I know that this whole program that we have developed has been aided by other people's efforts in the area. This is not something that we have invented completely on our own. It is a joint effort.

Ms. ENNIS. Senator, if you do not mind, I have something, if I could add to that.

Senator HAWLEY. Please.

Ms. ENNIS. We have coordinated closely with the Treasury Inspector General's office and learned from their playbook. The online form that the agency helped us develop was right out of their playbook.

I will say some of the other efforts they have done, which I do not want to reveal, worked for them, but the scammers are very inventive, and the minute something works, they change, and it is sort of playing catch-up a lot, so what worked then, it may not work again today, and so we are trying to always stay ahead of it, but it is difficult.

Senator HAWLEY. Very good. Thank you.

Ms. Ennis, while I have you, let me ask you a couple of questions. Let me go back to the subject of telecoms, which Senator Collins raised, which I thought was such an important topic. Is there more that we need to do, Congress needs to do, in order to enable partnerships, productive partnerships with the telecoms? They seem so vital to this.

Ms. ENNIS. Well, I do know—if you look at the complaints yesterday, the telecoms—besides what I talked about with the major telecoms, what they were also helpful with was some of the major ones put on notice that the companies that were the subject of the complaints yesterday, looking at the traffic and noticing certain patterns in the traffic and put them on notice. They should continue and hopefully will continue to do that because notice is a helpful thing from a legal perspective when companies do receive notice. Then they cannot say, "We did not know." They have been helpful in that regard too.

I am not an expert in the law related to telecoms, but I will say something, I think, to hold the gateways accountable would be something that we would look to that they should know their customer. Call duration and hang-ups in huge volume, like we have seen with this, you will see in the complaints, is a huge red flag. They have to be charged with looking at the red flags and knowing who is behind that, and instead, it seems as though they are able to turn a blind eye. I would hope that you could look at that, and we will be happy to provide any information we can, should you be able to do something in that regard.

Senator HAWLEY. That is very helpful. We will followup with you about that.

Let me ask you, finally, in my prior capacity as Attorney General of the State of Missouri, my office received numerous complaints about Social Security impersonation scams. I am just wondering to what extent the Social Security Administration has or is coordinating with State Attorneys General or other law enforcement officials.

Ms. ENNIS. Well, that is probably an area we should look into more, frankly. We have been partnering with other Federal partners, and there are many individual cases around the country where local law enforcement get involved or local State Attorneys Generals. We probably could do a better job at that, and thank you for identifying that as a place that we can partner up. We are always looking for partners, as I said, to extend our forces. We will look at that. Thank you.

Senator HAWLEY. Thank you, Madam Chair.

The CHAIRMAN. Thank you.

Senator Blumenthal?

Senator BLUMENTHAL. Thanks, Madam Chair, and thank you for having this critical hearing. We all know from seniors how robocalls, spoofing, phishing, all of the techniques apply to so many other consumer areas also are used in this one, like Senator Hawley as a former Attorney General, protecting consumers, particularly seniors against these kinds of scams can be a life's work.

I introduced Social Security 2100, which provides far-reaching reforms, along with Senator Van Hollen and my colleague from Connecticut, John Larson. These kinds of reforms are absolutely necessary to make the cost-of-living adjustment formula realistic, so beneficiaries can actually get the benefits that are more comparable, the costs they face today and additional benefits for Medicaid and other programs are not held against them, and the bill would keep the program solvent through the end of the century, ensuring security for Americans to come.

I have also included in this bill, measures to assure protection against these kinds of scams, and I think particularly in the area of enforcement with respect to laws on the books as well as new laws, enforcement is critical.

Yesterday the Department of Justice, as I think may have been raised already, in conjunction with the Social Security Administration, the United States Postal Service, and others, announced their first enforcement action against telecommunications companies operating in New York and Arizona who were facilitating robocalls in India. The Department of Justice is attempting to block these telecom companies from making or facilitating future calls.

I wonder if each of you could comments on the efficacy of current enforcement and what needs to be done to improve it.

Ms. ENNIS. Thank you, Senator.

I think right now, yesterday, there were several actions. We still have ongoing investigative work in conjunction with our Federal partners, so we are hopeful that there will be more coming down the pike.

As I have talked about the gateway carriers, though, I think there is room to do something legally there, whether it is legislatively or otherwise, because they tend to have ignored, turned a blind eye to what was obvious when looking at traffic patterns, so I think there is a gap there.

I think the TRACED Act and all of the proposed legislation that is out there, all will help move the ball forward in trying to combat these scams, but at the end of the day, it is still about educating and public awareness because, as I have said, the scammers are very creative, and the minute we plug one hole, frankly, they will find another one. While all efforts that you can make will be welcomed by us and our Federal law enforcement partners and State and local as well, the best thing for us to do is to educate the public.

Better coordination among Federal agencies is what has happened to allow what happened yesterday to occur, and anything that we can do to facilitate that is also very helpful. It is a force multiplier for a small agency like mine, and there is expertise with-

in the Federal Government, and it brings all that attention to these issues, and that is a wonderful thing as well.

Mr. SAUL. Just following up on that, the education part of this and the outreach is probably the most important and effective way to bring this terrible problem under control.

I have outlined in my report, which you have a copy of, the efforts that we have taken here, and we have attacked just about, I think at this point, pretty much every media, social media, into that, whatever we can do to get our message out to our people, to our customers. That is my responsibility as the Commissioner to be sure that we have turned every rock over, to be sure that we are effectively communicating with our customer.

I think if you look at the program, which we did not have, Senator, in the beginning, over the last 6 months, I think we have vastly improved our outreach. Any comments, of course, we would like to hear, but I think over the next months as this rolls out even further, we are on the right track now of really educating our customers.

Senator BLUMENTHAL. Thank you both for your testimony. My time has expired, but I think really a full-court press on increasing the resources for enforcement is vital because we all know the best laws on the books are a dead letter if they are not enforced. Thank you both for your service.

Thanks.

The CHAIRMAN. Thank you, Senator.

Senator Sinema, welcome.

Senator SINEMA. Chairman Collins and Ranking Member Casey, thank you for today's hearing on protecting seniors from criminal fraudsters who impersonate the Social Security Administration.

When I was a member of the House, I was proud to have worked with Chairman Collins to pass the Senior Safe Act into law. It empowered financial institutions to report suspected instances of elder financial abuse, and this Congress, together we have introduced the Senior Security Act to create a task force at the Securities and Exchange Commission to protect seniors from financial crimes.

Soon I will be introducing the Improving Social Security's Service to Victims of Identity Theft Act, a companion to the bipartisan House bill introduced by Representatives John Larson of Connecticut and Tom Reed of New York. This bill will provide identity theft victims with a single point of contact within the Social Security Administration when a fraudster steals and misuses their Social Security number.

Rather than ask victims to retell their traumatic story to multiple employees, this assigned individual will be their trusted navigator across different functions within Social Security to ensure they are not fighting these battles alone, and I look forward to working with the Social Security Administration on this effort.

My first question is for Commissioner Saul, but I would welcome additional thoughts from Inspector General Ennis, if you have anything to add.

I wanted to share this story of a constituent of mine, Liz, who lives in Mesa, Arizona. In a single day, she received over a dozen unsolicited phone calls and threatening messages falsely claiming her Social Security number had been compromised and suspended.

The criminals sought to scare Liz into divulging her bank account information. Luckily, she recognized this was a scam, but she is sharing her story because she is worried that not everyone would recognize it.

Identity theft and scams can be devastating, which is why I have previously worked with Senator Tim Scott on the Protecting Children from Identity Theft Act and with the Social Security Administration to help families whose children's Social Security numbers had been compromised, back when I was Member of the House.

In cases where people have been scammed, on their ways to help them financially recover, to secure their identities after their personally identifiable information has been compromised, and if not, what barriers prevent people from getting some of their life savings back or being able to secure their identities again?

Mr. SAUL. Senator, we are obviously facing a really serious problem here, and I do not think there is a really simple answer.

I know it would be easy to say, "Here is what we are going to do, and we are going to make everybody whole and do everything," but it is not realistic.

Again, I go back to the education process, which I know it sounds very simplistic, but I do believe in the end to make our customer and our beneficiaries aware of what is going on is really going to do the most for identity theft and all the terrible issues you have brought up.

I want to tell you one thing, though. One of our major efforts that is under way right now is individual identity recognition. We have to do a much better job in affording our customers the ability to have identity recognition, and it is something we are working on. It is not easy because of all the legal restrictions we have, but over the next year or two, I do believe you are going to see individual identity recognition rolled out in our agency in a very, very efficient manner.

We are right in the midst of working on it, and it is very exciting. I think that will also help tremendously in the issues that you have raised, so we are very aware of it. We are going to be putting a tremendous amount of resources into developing the proper individual recognition systems.

Senator SINEMA. Thank you.

Ms. ENNIS. To follow on that, I think the ubiquitousness of the use of the Social Security number as a form of identity in every element of your life—I know we are trying to change that. The faster we can change that, the better we will be off for everybody. That number should not be used as a form of identification.

When I was in college, I remember you used to print it on the face of your check, so we have changed. We have gotten better about that, but we really still use it every day you transact in your life when someone is asking for your Social or last four digits, so that would go a long way, I think.

Restitution will play it out. You know, if we are able to do things investigatively and with enforcement efforts, of course, we can seek restitution from bad actors.

If there were civil forfeiture for agencies where fraud is the crime, we could look to have a victims fund to, hopefully, try to re-

store some of those funds. Those are some of the things we talk about from an enforcement perspective.

Senator SINEMA. Thank you so much.

Chairman, thank you for hosting this important discussion today. I yield back.

The CHAIRMAN. Thank you very much.

Senator Gillibrand?

Senator GILLIBRAND. I just want to thank the Chairwoman and the Ranking Member for this hearing. We have been tackling this issue in New York State constantly. I cannot tell you how many scams, how many seniors are robbed of all of their savings, of everything they have left, devastating their families, and I have talked to law enforcement and I have talked to our Federal agencies. No matter how many reforms they put in place, the problem continues to rise.

We now have international networks coming from Russia, coming from Europe, coming from all over the globe trying to attack our seniors because they have a lot of wealth. I think seniors have over a trillion dollars in savings, so it is just a great source of money for them to scam out of Americans.

Mr. Saul, just a couple questions. What have you seen? What successes have you seen in combating scams, fraud, and financial abuse of older adults? What are the biggest challenges you face right now, and would better coordination between agencies in the development and implementation of new educational standards help? That is something that Senator Collins and I are working on right now.

Mr. SAUL. I think we need all the help we can get to educate our customer and to educate the American public, so whatever you all can do, I am all for it.

As I said in my statement—and we have talked about this, this morning—we have rolled out, I think, a pretty comprehensive program of educating our customer and our beneficiary through the help of a lot of media, a lot of outside organizations, plus our own internal communications. It is never enough. I mean, whatever help we can get, it is a continuing process.

We are in the initial phases, I believe, of educating our people. In my statement, you will see where we have outlined pretty extensive detail, our current efforts. I would appreciate any comments, any Senator, of course, has or any of the staff, but I do think at this point, it is a matter of time now to roll out the initiatives that we have begun. I do think they will make a big difference in educating the American public.

Senator GILLIBRAND. Thank you.

I want to talk to you about a broader issue, since we have you, about cutting Social Security benefits. I had the pleasure of traveling all across the country, because I was running for President for about 8 months, and I got to talk to people in Iowa. I got to talk to people in New Hampshire and Michigan and Pennsylvania and Wisconsin, and I can tell you, they believe that Social Security is vital to their life-and-death survival.

I saw the need for both our seniors and for people with disabilities, and I would really like to work with the Committee and you on ways we can shore up Social Security.

I was very worried when I heard from President Trump that he was thinking about cutting Social Security and other safety net benefits. That was shocking to me, given all of the things I have heard across the country.

I was also interested in assessing how we can help people with disabilities, and this might be a subject for a hearing, particularly the caregivers. I was wondering, have you ever investigated whether or not you think it would be an appropriate benefit to get the minimal benefits for Social Security and people with disabilities up to about on average $1,500 a month? Second, would you consider ever allowing Social Security benefits for full-time caregivers?

Mr. SAUL. I think that I take my responsibility as awesome. The Social Security Administration really affects more people in this country than anything, ex the military. I always say that. It is the most important thing there.

We support almost 100 million people every single month, and some of these people depend on this to buy groceries, as you say.

Senator GILLIBRAND. Everything.

Mr. SAUL. Right. Half the people that receive old age survivor's benefits have virtually no other savings, no other income, and without this support, they would be finished. They would be really in serious trouble. I want to assure you I take this responsibility very seriously.

I feel we need to do everything we can to shore up the Social Security system. I leave that to you guys. I mean, it is legislative responsibility, and I really mean that.

My job here is to be sure that with the resources that we have, we deliver them in the most cost-effective, best way we possibly can. I am here to serve the beneficiaries and our customers. Since I have been here in June, that is our mojo. That is our motto. Every decision we make is to serve the beneficiaries, and I really mean that.

Senator GILLIBRAND. Thank you for your service, and thank you for your testimony.

The CHAIRMAN. Thank you, Senator.

Senator Rosen?

Senator ROSEN. Well, good morning. Thank you for being here. Thank you, Senator Collins, Senator Casey, for holding this hearing.

It is pretty funny. I want to say it is funny in a ha-ha way, but the topic at hand, I will tell you just a couple months ago, I was on the Senate floor. I walked into the cloak room to answer a call that I thought was from a number that I knew, and sure enough, I am a Senator in the Senate cloak room getting told that my Social Security number is suddenly being deactivated, whatever the language that they are using. I think that was the week that we passed the robocalls or introduced that. It is pretty ironic that even Senators get these calls when we are here doing this. We could be having them on our phones as we speak. Of course, I am by no means the only Nevadan, the only person in the country targeted by these, and Nevada, unfortunately, has the most cases, most reported cases of fraud per capita, about $15 million in losses a year, and the fifth most cases of identity theft—Senator Sinema was talking about—with over 7,500 cases reported last year.

You just mentioned you touch 100 million people every month, and so as a former systems analyst, I was thinking about how we could plug in. This is kind of a two-part question for both of you.

We have some existing infrastructure—our banks, our credit card companies. I wrote some of those programs, robust fraud programs. How could we take the statistics that we know on this, plug into their existing infrastructure to warn, identify, let people know?

Second, we know that seniors probably get most of their bills, I would suspect, in the mail. They are utility bills, okay? Every month, you get an electric bill, and there are ways to put little fliers, things in there that are instructive that a senior who may not be using the internet may not be capable because of age or disability, but everyone is usually paying an electric bill, I would say, water bill, gas bill, whatever, public utility bill. Are there some ways in our national infrastructure that we can connect with this nearly 100 million people every month that you are touching already?

Mr. SAUL. I want to assure you that we are in constant communication with our beneficiaries.

For example, we just came up—as far as the scam and the fraud which I outlined in my initial remarks, we came up with a way that all our mailers now on the outside of the envelope, just something you are referring to, is going to have the scam message printed, affixed to the outside of the envelope.

When you get a normal statement, COLA statement, something like that, you are going to get a scam notice because when you go to open up the envelope, right smack in your face is going to be our scam notice, "Beware"——

Senator ROSEN. Right, but maybe there is other partners——

Mr. SAUL. I am sorry?

Senator ROSEN [continuing]. other family members out there, partners in the community that would be helpful to use this too.

Mr. SAUL. Whatever we can do. Look, this is an ongoing thing, but we are coming up constantly with new ways to be able to communicate with our customers.

As far as using the banking system and the other private-sector corporations, we have an act that we are partnering with all the financial—not all, but the financial institutions and banks, as we speak. We are rolling it out in June——

Senator ROSEN. Fantastic.

Mr. SAUL [continuing]. where we are going to verify the Social Security identity numbers for the institution. If somebody comes in applying for credit using a Social Security number, we will verify for that institution that they are legitimate, so, yes, we are working.

Senator ROSEN. That is fantastic.

Mr. SAUL. As a matter of fact, this is a major roll-out force that has been done with consultation with legislation and consultation and participation by the financial industry. Those banks are actually paying for the technology to support this endeavor.

Senator ROSEN. That is a great idea to think of ways we can partner and streamline.

Mr. SAUL. There is a lot of things happening. I do not know if you were here when I spoke initially. Individual identity is going

to be one of the most important technological things that you are going to see come out of the Social Security Administration in the next 2 years. We are going to be spending a fortune on this to develop a really proper individual identity.

It looks like it is going to be through the use of driver's licenses. We will hear more and you will hear more about this over the next 6 months to 9 months as we roll this out, but it is one of my priorities, so there is a lot going on in this area. You are absolutely right to bring it up, Senator.

Senator ROSEN. Thank you. I think I am out of time, unless you want to let her answer.

Ms. ENNIS. We are just partnering with the United States Postal Inspection Services for a co-branded poster that is going to go in post offices around the country to warn about scams generally, and we have reached out to other retail partners, but to your suggestion, there are probably other utilities and other infrastructures that we can continue to reach out to. Again, it is about resources to try to do that, but we are working that way with retail banks, financial institutions, and with educational materials as well.

The CHAIRMAN. Thank you very much.

I want to thank our panel of witnesses—the Commission, the Inspector General—for all the work that you are doing and for sharing with us your ideas. We look forward to continuing to have a close partnership so that we can put an end to this pernicious scam that is costing so many of our vulnerable seniors literally their life savings. I thank you for your commitment, for the actions that you have taken and for being with us this morning.

I would now like to call forth our second panel of witnesses. First, we will hear from Machel Andersen, who joins us from Ogden, Utah. Ms. Andersen has courageously agreed to testify today about her personal experience with the Social Security scam. She is accompanied by her husband, Utah State Representative Kyle Andersen.

The second witness that we will hear today is from the great State of Maine, Justin Groshon. Mr. Groshon manages the Social Security field office in Saco, Maine, and will testify today on behalf of the National Council of Social Security Management Associations, which represent Social Security field office managers throughout the country. He has served the Social Security Administration since 2004 and has managed the Saco field office since 2011. We are very grateful for your service and for your being here with us today, Justin.

Finally, I will turn to our Ranking Member to introduce our witness from the Commonwealth of Pennsylvania.

Senator CASEY. Thank you, Chairman Collins.

I am pleased to introduce a good friend of mine, Nora Dowd Eisenhower, who is also a great friend to seniors in Pennsylvania. She comes from southeastern Pennsylvania. I come from the northeast, about 2 hours north, but I have known Nora for many years, and for more than just a few years, she has been working on aging policy. She currently serves as the executive director of the Mayor's Commission on Aging in the city of Philadelphia. Previously, she served as assistant director for the Office of Older Americans at the

U.S. Consumer Financial Protection Bureau and was the Secretary of the Pennsylvania Department of Aging.

Nora brings a wealth of experience to her testimony before this Committee, and I have known both Nora and her husband, Jim, for many years. I am grateful they are here—she is here today.

Nora, thanks for appearing.

The CHAIRMAN. Thank you.

Ms. Andersen, thank you so much for being here today.

STATEMENT OF MACHEL ANDERSEN, VICTIM OF THE SOCIAL SECURITY IMPERSONATION SCAM, OGDEN, UTAH

Ms. ANDERSEN. Chairman Collins, Ranking Member Casey, and distinguished members of the Committee, thank you for the opportunity to tell you how international criminals used the Social Security scam to steal $150,000 from me and my husband, money we had worked our entire lives to save.

This terrible story began on Friday, December 6th. I was busy and distracted that day because one of my daughters had just had surgery, and I needed to help with the grandkids. At some point, I noticed I had missed three automated voice-mails from what appeared to be the Social Security Administration with messages telling me that my Social Security number had been compromised.

When I called back, a man who claimed to be Joseph Gangloff answered. He told me he was with the Social Security Administration. He gave me his badge number, and he told me that I was to look him up online. I would find out he was the Chief Counsel to the Social Security Administration. Then he told me some bad news. A car registered in my name was found with blood all over it at a crime scene near the Mexican border. Worse, he said that my Social Security number had been used to set up multiple bank accounts associated with a drug cartel, and he then transferred me to someone who claimed to be a DEA investigator named Uttam Dhillon.

This man told me that my family was in danger, that my Social Security number was being used by a very powerful drug cartel, and that they would be watching my every move. He said that any accounts associated with my Social Security number would be seized as part of the DEA investigation, and that to protect our money, I would need to transfer all of it to a safe offshore account. He said that if I cooperated, I would receive a new Social Security number and get all of our money back, but if I did not, I could be suspected of working with the cartel. He insisted that I act normal and not tell anyone, and he reminded me that both the bad guys and the Government were watching everything I was doing.

By the time I arrived at the credit union, it was too late in the day to send transfers overseas, but I was able to combine all our resources into one account. That weekend, I called the scammer back to see if there was some other way to handle the situation. He said the only other option was my arrest.

Monday morning, I went to the other financial institutions where we had accounts to transfer all our money to Hong Kong. The scammer insisted that I keep him on speakerphone the entire time. I was in the credit union, so I put the phone in my purse. When the clerk asked why I was sending so much money overseas, I said

that it was for electronics, just like the scammer told me. That was the only question I was asked.

Ultimately, I sent $154,646 in two transfer to Hong Kong. In hindsight, I realize there were many signs that I should have recognized indicating that I was being scammed, but the scammers had me so worked up. They told me that I had to be convincing or I would end up getting arrested. They even sent me fake arrest warrants.

I also wonder why my financial institution did not ask more questions when a longtime customer who had never executed a wire transfer suddenly cashed CDs for which penalties were charged, deposited large amounts of money from other institutions, and transferred almost every dollar she has in that institution to a bank in China to buy electronics.

Having our life savings stolen has made me realize there are some very bad people in this world, but losing this money has also reminded me that my life is rich in many ways. I live a wonderful life in a wonderful place. I have a great husband and great family. I am truly blessed.

Maybe hearing my story will help protect some other family that would have had a harder time recovering from something like this. Maybe my story will help these scammers stop, once and for all. I hope so.

Thank you for allowing me to tell my story here today.

The CHAIRMAN. Ms. Andersen, before we go on to the next witness, I want to thank you for your courage for coming forward and publicly describing what happened to you, and I can assure you that you personally are going to be responsible for many other people not getting scammed because they will recognize the signs due to your courageous testimony.

I know it took a lot to come forward and tell what happened to you, but you have done such a public service. You will save so many other people from going through the terrible scam that robbed you of over $154,000. I just wanted to thank you before we moved on.

Ms. ANDERSEN. Thank you, Chairman Collins. I hope so.

The CHAIRMAN. Thank you.

Mr. Groshon, welcome.

STATEMENT OF JUSTIN GROSHON, MANAGER, SACO SOCIAL SECURITY OFFICE, SACO, MAINE, APPEARING ON BEHALF OF THE NATIONAL COUNSEL OF SOCIAL SECURITY MANAGEMENT ASSOCIATIONS

Mr. GROSHON. Chairman Collins, Ranking Member Casey, and members of the Committee, my name is Justin Groshon, and I am the district manager of the Saco, Maine, Social Security office. I am also the president of the New England Social Security Management Association and an executive committee member for the National Council of Social Security Management Associations.

On behalf of the National Council and my colleagues back home in Maine, thank you for the opportunity to be here today to discuss Social Security impersonation scams.

In October 2019, our National Council conducted a survey on the various SSA impersonation scams and the impact on Social Security field offices and teleservice centers nationwide. We received re-

sponses from over 500 managers and supervisors on the impact to their respective offices. Over 97 percent responded that their office had received reports from the public about callers impersonating a Social Security employee. Of those, almost 70 percent reported that this was a daily occurrence, with 50 percent reporting as many as 15 contacts per day.

In my home State of Maine, all of our field offices have been impacted by SSA impersonation scams. Every day, our offices assist callers and visitors reporting Social Security scams. In many instances, the impersonators appear legitimate to their victims as they spoof or mask the phone number they are calling from with an actual Social Security field office phone number.

After receiving the impersonation call, a large number of people contact our offices in an attempt to verify the authenticity of the call. In some instances, this leads to increased call volumes of 400 percent to 1,000 percent. The increased call volumes prevent our agency from being able to conduct legitimate business with those seeking our core services.

For one Maine office, this increased call volume lasted almost 22 days. Ultimately, that office was forced to change its phone number.

Consistent with information shared by the Social Security Administration's Office of the Inspector General, the people contacting our offices indicate that the impersonators threaten them with legal action, fines, arrest, or make promises for increased benefits.

There are other ways the scammers have impacted our ability to serve the public. Several offices have reported receiving automated robocalls to their phone lines inundating their phone system with threatening messages similar to those received by our customers.

In one day alone, an office received almost 2,000 automated calls to the Office General Inquiry phone line, and during that time, the office was unable to serve its actual customers by phone.

In my own office, the General Inquiry telephone line, the number I rely on to serve the public was used in automated call scams. These scams occurred on three separate occasions, each lasting 3 days. This significantly reduced our ability to serve the public and degraded the services to the residents of York County, Maine.

Today we have heard from an individual directly impacted by these scams. Her story should not be considered an isolated incident. It has become an unfortunate reality for our field office employees to hear from new victims each week. Their stories have become all too common.

These rampant fraud schemes are not isolated to Maine. They are prevalent throughout the United States, and our colleagues from all 50 States have experienced similar issues. Managers and supervisors in offices across the Nation have expressed the same concerns as my colleagues back home.

It is important to note some of the feedback our managers provided describing additional implications of Social Security impersonation scams. First, employees conducting legitimate Social Security business have been met with suspicious leading to repeated telephone calls, the need for members of the public to visit our office, and delays in processing claims in other post-entitlement work.

Second, some customers are convinced that Social Security employee are behind the scam calls and, thus, view our staff with distrust. This further erodes the confidence the American public has in our agency and the Federal Government as a whole. That said, our employees will continue to do their best to assist our customers with questions and concerns related to the scam calls.

On behalf of the National Council, thank you for the opportunity to be here today. We want to ensure that Maine residents and the American public have faith and trust in the Social Security Administration and that they are reassured that they will not fall victim to those trying to impersonate SSA employees.

We respectfully ask that you consider our comments and appreciate any assistance you can provide in ensuring the residents of Maine and the rest of the American public receive the critical and necessary service they deserve from the Social Security Administration without fear of compromising their information.

We greatly appreciate the Committee's focus on these very important issues, and I will be happy to answer any questions you may have at that time.

The CHAIRMAN. Thank you very much.

Ms. Dowd Eisenhower?

STATEMENT OF NORA DOWD EISENHOWER, EXECUTIVE DIRECTOR, MAYOR'S COMMISSION ON AGING, PHILADELPHIA, PENNSYLVANIA

Ms. DOWD EISENHOWER. Good morning, Senators, and a special thank you to Senator Casey for inviting me to speak today.

As a government official and public interest attorney who has advocated for older Americans for more than 30 years, I am pleased to present today some ideas for reducing the vulnerability of older Americans to the Social Security impersonation scam.

I am a proud Philadelphian and appreciate Mayor Jim Kenney's leadership in improving economic opportunities and public safety for all Philadelphians. Senator Casey and Senator Collins and this Committee continue to shine a light on the critical needs of older people in our country. We are proud to have Senator Casey represent us in Washington on this important Committee.

I am the executive director of the Mayor's Commission on Aging in Philadelphia, where almost 295,000 older adults live and work. Locally, nationally, and globally, people are living longer. The longevity bonus demands a new approach to our way of thinking.

Philadelphia seniors are a diverse and culturally vibrant part of our neighborhoods, and many live with family and loved ones in multigenerational settings. However, nearly one in four, or 24 percent of older Philadelphians, living alone see friends or relatives less than once a week. This can lead to isolation and vulnerability and should be considered when developing interventions to help protect them against fraud.

Philadelphia is also home to the largest percentage of seniors and poorest overall population in the top 10 cities in the country.

I am not going to go into the Social Security scam again. I think we have it down. I think we realize that it is the latest variation on telemarketing fraud that we have all been working to prevent for many, many years, but I think that we need to look at some

of the solutions that have worked and in fact even look at the change in scams in the top 10 from the IRS scam to being No. 1, to the Social Security scam being No. 1 as a success story of sorts.

Many people now know that those IRS calls that have been coming in for years are phony. The same has not reached people about the Social Security scam, and in fact, I did not hear of it until I got a call from a Senator Casey staffer asking me to come and speak to this Committee. Of course, I did a little research, but I was not hearing about it on the ground in Philadelphia, where we run programs to support older Philadelphians in partnership with the Philadelphia Corporation for Aging.

We just went through the open enrollment season for Medicare where APPRISE counselors are talking to older Philadelphians every day about Medicare and what to choose, and often Social Security comes up.

I think while that was a missed opportunity, we certainly will be looking at the Social Security scam, looking at the materials, especially those materials created in partnership with the Federal Trade Commission, the Social Security Administration, and my former agency, the Consumer Financial Protection Bureau. They have already created an excellent piece. It is a one-pager. It is similar, Senator Casey, to what is in the back of your most recent report on fighting frauds. It is brief, it is concise, and it is really helpful. Now we need to get the word out.

I will recommend, though, also that we pass the Stop Senior Scams Act sponsored by the Aging Committee, sponsored by the Committee's Ranking Member Senator Casey and the Commerce Subcommittee on Manufacturing, Trade, and Consumer Protection, Chairman Jerry Moran.

The act recommends that an advisory council be created, that it collect and develop model educational materials for retailers, financial institutions, banks and credit unions, and wire transfer companies to share with their employees. Employees are often the front line, as we have heard from Ms. Andersen, that last moment in time when we could prevent that money from going abroad, never to be returned in many instances.

We can examine the ways these businesses can use their platforms to educate the public on scams. We can provide additional helpful information to retailers, financial institutions, and wire transfer companies as they work to prevent fraud affecting older adults. They need this information.

We can publicly report information about the newly created models as well as recommendations and findings of the advisory council.

I will say also we should look to successful models that are already out there. The CFPB created Money Smart for Older Adults in recognition of the reality that older adults have been and continue to be prime targets for fraudsters. Money Smart for Older Adults Version 2.0 is also available in Spanish. It raises the awareness of many common frauds and scams, and that is important because the scam today is Social Security, which is a terrible thing, but next year it might be something else and the following year something else again.

We need to have a mechanism in place to educate people about those scams as they are changing, faster than the fraudsters can change them. Outreach and education that the Federal Government is already funding, called Senior Medicare Fraud Patrols, are currently conducted in every State and could be replicated with a focus on Social Security scams. This will take resources. The SMP program model is one of prevention. SMPs have empowered Medicare beneficiaries since 1997 to scrutinize their medical bills and statements. The OIG reports that expected recoveries to Medicare and Medicaid attributable to the projects from 1997 through 2018 were over $100 million. Total savings to beneficiaries and others were approximately $7 million, but that is an undercount, I am sure.

I am grateful for your attention to this matter, and I thank you for the opportunity to speak with you about it. Other opportunities could exist with Meals on Wheels and area agencies on aging that are already communicating with older Americans, especially shut-ins.

Thank you.

The CHAIRMAN. Thank you very much for your testimony and your recommendations.

Ms. Andersen, in your written testimony, you mention that the criminals also tried, after they had received all of your life savings, to get you to remortgage your house. Could you tell us a little bit about that?

Ms. ANDERSEN. Yes. They called and asked if I had a mortgage on my home, and I said, "No. Our home is paid for. We have no mortgage," and he said, "That is what I was afraid of. We have got to secure your home before the seizure. We are going to need you to come up with 45 percent of the value of your home. What do you think your home is worth?" and I told him, and then he said, "That means you are going to have to come up with about $200,000, and you are going to have to get a mortgage." I said, "I cannot get a mortgage without my husband. In fact, I was so weary of all these calls and stuff that I began to laugh. I said, "That is really funny. I cannot do that," and he said, "Then you are going to have to find someone who can give you that money, or you will lose your home." I kind of just put it away because I was with the grandchildren. I was picking up one of them from preschool. I went about my day. He called again. I said, "You are going to have to seize my home. I do not have that kind of money. I do not know anyone who does," and he said, "No. You have got to start calling people. You will lose your home, and this is a serious threat." I thought I was talking to a DEA agent at the time. I said, "Okay." I hung up the phone. I called our best friend who I thought maybe would have that kind of money, and he said, "I do not have anything liquid right now. I am so sorry," and then called me back a few hours later and said, "I can get you $60,000 today. I can get you the other 140 on Monday." and I said, "Thank you." I had told him, "I cannot tell you what it is for. My husband cannot know. Your wife cannot know," and he was still willing to loan me that money. I am so grateful that I came to my senses and was able to look some of this up online before I went any further.

The CHAIRMAN. Did he ask you whether you might be being scammed?

Ms. ANDERSEN. My friend did. He said, "Machel, are you sure you are not being scammed?" and I said, "I am sure I am not. I am not being scammed."

The CHAIRMAN. Was that because you thought you were dealing with a DEA agent, with the Social Security Administration, with trusted Federal agencies?

Ms. ANDERSEN. Yes.

The CHAIRMAN. What do you think would have been helpful in stopping you right from the beginning?

Now, you were in a very stressful situation. Your daughter had had surgery. You were taking care of your young grandchildren. You had a lot going on in your life personally that was causing stress, but tell me what you think would have been most helpful. I know that at the credit union, they asked one question, and we passed a law that I wrote with Claire McCaskill—and Senator Sinema was helpful in the House—to give immunity to banks and credit unions so that they can ask those kinds of questions and not violate bank privacy laws. Do you think further questions would have been helpful? What do you think would have alerted you?

Ms. ANDERSEN. I do. I think that is the front line is the banks and the credit unions for that.

We have talked about it since. There were many signs that I was being scammed that in hindsight I can see now, but the bank would have been the front line for me because I watch very, very little TV. I very rarely listen to the radio. Maybe it sounds like I live under a rock. I do not know, but that is not part of my day.

The CHAIRMAN. You have a busy life.

Ms. ANDERSEN. Yes, yes.

The CHAIRMAN. I think all of us might be better off not watching television these days. That is a joke for all the news media here today.

Ms. ANDERSEN. Yes. If I had been asked more questions at the bank, I think that would have helped.

The CHAIRMAN. That is helpful to know because getting the word out is so important.

Mr. Groshon, you have given us a whole different picture today and a really important one. You mentioned that every single field office in Maine has had to deal with a flood of these calls, with spoof numbers. How many field offices do we have in Maine? Do you know off the top of your head?

Mr. GROSHON. I believe it is eight. Yes, we have eight offices.

The CHAIRMAN. It sounds like this was overwhelming their ability to carry out their day-to-day business, so enrolling people in Social Security, giving them advice, making sure they have the forms for Medicare. Is that accurate?

Mr. GROSHON. That is correct. We—yes. I am sorry.

The CHAIRMAN. No, go ahead.

Mr. GROSHON. It was to different degrees to different offices. I can certainly speak to Saco, Portland, Auburn had the most catastrophic of those instances that we described of spoof numbers where our numbers were used on the Caller IDs for individuals. When they returned phone calls, for all intents and purposes, it in-

undated the phone system, rendered them almost useful for the day as far as serving our actual customers in our local service areas.

The CHAIRMAN. You mentioned another fact which I think is really important is that this scam not only has hurt so many people nationwide, but it has eroded trust in Federal employees and those who are working so hard to serve the public. Could you talk a little bit about that as well?

Mr. GROSHON. Absolutely. There is a few different ways. I talked about delays in processing claims, and I think one good example is we are trying to get individuals that are capable of doing so to file certain claims online. Those claims sometimes require us to followup with them to just clarify some question or answer that they provided, and in many of those instances where we reach out to them by phone, they do not believe that it is actually us calling, even though they had just filed an application online the day before. Oftentimes that requires an in-person visit.

I will speak to, I guess, Maine or really anywhere that has large geographic areas or large service areas for our field offices. That can mean somebody is driving upwards of an hour, in the northern half of the State over 2 hours to their local field office to have an in-person interview that really was not necessary should we not have this other factor of the potential for a scam call, so that certainly is one way that that distrust is exhibited for us in trying to conduct actual business.

There are times when people mail us paperwork that needs a couple of questions answered, and again, we make phone calls. Even though we just received paperwork from this individual—they know they sent us something—they still do not believe that we are who we say we are, and that is a challenge.

Unfortunately for us, in order to identify you over the phone so that we can disclose certain pieces of information to you, we are going to ask you six what should be very private questions to you so that we can make sure that we are not disclosing information to somebody else, and obviously, that creates just a cataclysmic problem of we need to ask them certain questions, but they do not believe who we are and that leads to just extraneous contacts.

The CHAIRMAN. I think you have brought up a very good point that has not been discussed before, but think about it. If you see on your Caller ID that it is Social Security Administration calling and then the person is asking you for personal information, how is the average person—how is anyone going to be able to distinguish between whether this is a scam call versus a legitimate call from Social Security following up on a claim that has been filed?

Mr. GROSHON. That is a great question, and I can tell you as somebody who has received these calls myself—and somebody, again, working in the agency, sometimes I can ask questions, or I have been known to call them back. I receive these calls often enough that I will call a phone number that does not lead to a field office and does lead to somebody pretending to be in a field office somewhere, and we can ask certain questions about what office are you in and what phone number should I call or who else works in that office or some other questions like that. Typically, if you ask

enough questions, they will start to stutter, and so I think asking to call back, typically they do not have enough good answers.

That is not to say, as was pointed out, the level of sophistication that the individuals have described for this problem is more than I would have ever anticipated or imagined. This is not somebody just calling you on their own from their basement. This is a very well-organized attempt to steal your personal information or finances.

The CHAIRMAN. It is very sophisticated.

I have gone way over my time, but I am just going to ask you one more question before yielding to Senator Casey. I apologize, but I know we are going to be wrapping up the hearing. My question is, when someone does contact the local field office or comes in who has been targeted by a scam, what steps do your employees go through to try to assist them?

Mr. GROSHON. Again, this is where I think the problem—it will depend on exactly what their allegation is, did they actually become a victim to some kind of financial exploitation, in which case we directly refer them to local law enforcement, and then we also make our own referral to the Office of the Inspector General so that they have enough information that they can start to work with and contact that individual directly themselves for an investigative piece.

If it is just the case of losing personal information or identity information, we do make the referral to the individual, to the Federal Trade Commission, to the major credit bureaus to understand what things they can do to try to protect themselves, but at the end of the day, the fact that we use the Social Security number as a form of identity is a big problem, and unfortunately, a lot of those people come to us because they believe there is something we can do to help protect them, and there really is not a mechanism for us to do that at this point.

The CHAIRMAN. Thank you very much. Senator Casey, my apologies for going over.

Senator CASEY. Chairman Collins, thanks very much. We could spend a lot more time. We all wish we could, but I am grateful for the questions you asked. I am going to be following up on the first line of questioning.

I do want to start, though, with Ms. Andersen. I want to thank you for your testimony, your appearance here. As Senator Collins said, your example, your coming forward is going to help a lot more Americans and not just a few. Many.

I think we have seen in recent American history where sometimes one brave citizen coming forward demonstrating uncommon courage can really change the way we approach a problem, the way others will be inspired to be more aware, more vigilant. I just cannot even imagine what you had to ensure.

What jumped out of your testimony, I guess it was the third page of your testimony where you talk about your 7-month-old grandson with you in a car seat, and you had to haul the car seat into the credit unions. That kind of pressure and trauma, I think, demonstrated the kind of assault that you were enduring. We are grateful that you are willing to talk about it.

Ms. ANDERSEN. Thank you.

Senator CASEY. One point that you made in your testimony on that same page and in light of Senator Collins' question about the credit unions, the bill that Senator Moran and I have been working on got through his committee. It helps sometimes when the Committee chairman is working on a bill with you, but we are trying to get it through the whole Senate. One of the things we are trying to do there is to provide an opportunity for more training for those who work in credit unions, retailers, banks, and the like.

I am assuming that part of the response to what you had to live through was that kind of legislation. There may be other ways that you can provide help, not just on a bill like that, but for other strategies as we go forward. I just want to commend and salute your work and taking the time to be here.

Ms. ANDERSEN. Thank you.

Senator CASEY. In light of that, I want to turn to Nora Dowd Eisenhower about the bill.

Nora, in light of this testimony and also anything else that you want to add to the list or the itemization of the solutions in addition to the bill, my bill that you spoke about, anything else that you think we should be doing?

One thing I broadly will say is we are trying to do everything we cannot to just simply focus on retribution, because if we do that all day long, we will not get to prevention and all of that.

Wow. When I hear Ms. Andersen's story, you want to just seek vengeance, as we should. That is what law enforcement is for, partially, and sanctions. I hope that anyone who engages in this kind of conduct can go to prison for not years but decades. In addition to that, I hope that we can share some stories about what works, what does not work, and other solutions. If you are anyone else on the panel wants to speak to that before we wrap up?

Ms. DOWD EISENHOWER. I think aggressive enforcement is critically important. I think we all agree with that. It is hard to sit by and hear Ms. Andersen's story and not want to throttle someone. It is just terrible.

We have been successful in the past working together across disciplines, in the public sector and the private sector, in educating people. 10,000 people a day turn 65 in this country and are relying on the Social Security Administration to help them through that process of do I claim for Social Security now or do I wait later. It is a critical time in our country.

The fact that Social Security is now being used as the key imposter scam means we really have to pay attention to it. I know I will. I know I engage with older people across Philadelphia.

We are at the Firehouse Senior Center recently in West Philadelphia. That is the vulnerable population that I am most concerned about. They rely on Social Security. Some may be isolated—and this term "isolation," really not having engagement with the world as much as others do—and they may be even more vulnerable. I think it is something that we really need to work on.

I really love what you are trying to do in the Stop Senior Scam Act because it brings people together. It helps us engage not just in education, but in education of the financial institutions.

You and I know that that individual now who worked at that bank that Ms. Andersen went to is going to have that on their con-

science. I am sure they know about it now. It is not good for the financial institutions either. They want to educate people; they want to stop scams. We really need to help them and provide them with that, and partnerships are a key way to do that.

Senator CASEY. Anyone else? I know we have to conclude.

Mr. Groshon?

Mr. GROSHON. I think on behalf of the Management Association, we would agree that public awareness is critical to this, and anything that can be done is helpful, and I mean anything. There is still a number of people that just are not aware that this is going on.

Thank you.

Senator CASEY. Thanks very much.

Ms. DOWD EISENHOWER. Thank you, Senators.

The CHAIRMAN. Thank you, Senator Casey.

It is evident from hearing the two panels today and our excellent witnesses that combating these scams is going to take a coordinated all-hands-on-deck effort, and that is what we are committed to doing.

We will, as I mentioned, be releasing our annual Fraud Book, and it has tips for seniors. Like Senator Casey, I try to get these into senior centers all over the State of Maine. Area agencies on aging are also helping distribute them, as is AARP.

If we can heighten public awareness, we can prevent people from being victimized, but I do not think we should underestimate the ruthlessness, creativity, and pressure tactics that are used by these criminals. I call them "scammers" I call them "fraudsters" but, in fact, they are criminals. They are stealing money and personal information, and that is just so troubling to me.

This hearing is the 25th hearing that our Committee has held on scams that target seniors, and that ought to tell you about our commitment to stopping them. It also ought to tell you about the infinite variety and the persistence of criminals who perpetuate these scams.

I am pleased to hear today that the Social Security Administration and the Inspector General are working with Government, with law enforcement, with industry partners, with consumer groups like AARP to raise public awareness and disrupt attempts that are in progress.

Ms. Andersen, I will tell you that there is nothing more effective than for people to hear a firsthand account from someone who is just like them, and that is the most effective means of education.

I commend the Department of Justice for taking enforcement action. For many years, the Department of Justice said, "Well, these are too small dollar individually," when in fact, the latest statistics show that seniors are losing close to $3 billion a year to the se pernicious scams. Again, I think that is the tip of the iceberg because many of these scams and losses are never reported to law enforcement.

I hope that we are also encouraging more people to come forward, to report to law enforcement. Our Committee has a fraud hotline, and as I said at the very beginning, this Social Security scam is now the No. 1 reported scam to our hotline. We are going

to continue our educational efforts, our legislative efforts, and our attempts to encourage further law enforcement.

Just one final point on law enforcement, a lot of times, as we have learned, these gateway communication companies are very small. They are easy to put together, and they are hard to locate. Another problem is the scam may actually originate overseas. In fact, India has been a source of call centers for these scams, and thus, we have to have Federal law enforcement involved in order to close down those overseas call centers. That is really important as well.

Together, we are determined to continue to work with all of you to fight these ruthless criminals who are targeting our Nation's seniors and often those who are most vulnerable, who are living on their Social Security checks, who have very little by way of savings.

Senator Casey, do you have any final comments you would like to make?

Senator CASEY. Just briefly. Thank you, Chairman Collins. I want to thank you for this important hearing. I want to thank our witnesses.

We have heard today how ruthless—and that is probably an understatement—these scam artists can be. We all have, especially elected officials, a sacred duty to continue our work to protect seniors against these "criminals," to use the word that Senator Collins used. It is an important word to use in this context, especially when these criminals represent themselves as the U.S. Government.

I am glad that today we are releasing our 2020 Fraud Book. That gives seniors important information about these scams.

We know that this kind of information alone will not solve the problem. We have got a lot more work to do, as I mentioned my senior scams bill that will help better prepare and train retailers, banks, and wire transfer companies who are involved in the fight.

Chairman Collins, I want to thank you and our witnesses for making it possible to get this word out today. Thank you.

The CHAIRMAN. Thank you.

In addition, I want to thank our hardworking staff who put together this hearing and identified witnesses. They are very committed as well, and I thank them.

Committee members will have until Friday, February 7th, to submit additional questions for the record. If there are any, we will forward them promptly to you.

Thank you again to all of our witnesses and all the Committee members who participated in the hearing today. The fact that we had so many members drop by at such a very busy and intense time for the U.S. Senate speaks very well to the commitment of members to helping in this effort to halt these scams.

This concludes the hearing.

[Whereupon, at 11:59 a.m., the Committee was adjourned.]

APPENDIX

Prepared Witness Statements

SPECIAL COMMITTEE ON AGING

UNITED STATES SENATE

JANUARY 29, 2020

STATEMENT FOR THE RECORD

ANDREW SAUL
COMMISSIONER
SOCIAL SECURITY ADMINISTRATION

Committee Chair Collins, Ranking Member Casey, and Members of the Committee:

I am Andrew Saul, Commissioner of the Social Security Administration (SSA). Thank you for inviting me to discuss the phone scam crisis. I am deeply troubled that crooks are harming Americans and I am eager to discuss with you how we can protect the public.

The Problem

As a nation, we have come to realize the value of personal information and the damage that happens when that information lands in criminals' hands. To be clear, the scams we are discussing today are not Social Security program fraud. Rather, they are schemes to trick people into thinking a credible organization—a bank, a utility company, a credit card company, or the government, including SSA—is calling so that they give up their personal information, pay money, or both.

There are many variations. Scammers play on emotions like fear to get people to act without thinking. For example, a caller may say he is from SSA and that your Social Security Number (SSN) is suspended or has been used in a crime. The caller identification may be spoofed to appear to originate from a government number. The caller may ask you to provide information like your SSN to reactivate it. The caller may tell you your bank account will be seized and direct you to send money or gift cards for safekeeping. If you comply, your money is gone. If you don't comply, the caller may threaten you with arrest.

Although our programs—our core mission—are not the target of this fraud, SSA must share responsibility to help. Our programs require the public to interact with us. We cannot afford to have fraud affect that communication or the public's trust in us. Additionally, these schemes have caused a significant workload for SSA, such as increased calls to our National 800 Number (800 number) and fraud referrals, as well as our Office of the Inspector General (OIG). We must apply resources to this problem, which diverts time and employees from other critical workloads.

Our Agency

For almost 85 years, Social Security has provided vital benefits to the public, particularly our senior citizens. In Fiscal Year (FY) 2019, we paid over $1 trillion in benefits to approximately 70 million Social Security beneficiaries and Supplemental Security Income recipients. As of June 2019, approximately 88 percent of seniors age 65 and over received Social Security.

Our employees help millions of people. In FY 2019 we:

- Processed over 17 million applications for original and replacement Social Security cards;
- Posted 288 million earnings items to workers' records;
- Handled over 33 million calls on our 800 number;
- Helped 43.2 million visitors in field offices;

- Mailed nearly 255 million notices;
- Processed over 184 million online transactions;
- Completed over 7 million claims for benefits;
- Completed over 713,000 continuing disability reviews and nearly 2.67 million non-medical redeterminations of eligibility; and
- Provided access to the Social Security Statement, mailing over 11 million paper Statements and allowing individuals to access their Statements online more than 56 million times.

Few government agencies touch the lives of as many people as we do. Americans trust our agency and our employees, and we cannot allow swindlers to erode that relationship.

How We Are Helping

Phone scams have been around for several years and the agency initially responded with steps like sharing OIG Fraud Advisories and creating training videos for representative payees who help beneficiaries manage money. As these scams evolved and became more common, the agency took additional actions to:

- Collaborate with our OIG and major phone carriers to block[1] nearly all calls that attempt to spoof our published toll-free phone numbers from ever reaching the public;
- Distribute television and radio public service announcements throughout the country, issuing a national press release, and posting warnings on social media;
- Collaborate with OIG to display information on video monitors in 2,100 Walmart stores nationwide;
- Collaborate with the Consumer Financial Protection Bureau to help educate consumers on how to avoid Social Security scams;
- Share articles and guidance with the Centers for Medicare & Medicaid Services, ADvancing States, and the Senior Corps, as well as Social Security advocates, and third-party groups and organizations; and
- Offer a voice verification option to people who call our 800 number, which allows the caller to record their first and last name. When they receive a scheduled callback, callers hear their own voice, so they know the call is from us.

Upon becoming Commissioner, I quickly realized the magnitude of these scams and that SSA needed to take more aggressive action to address the scams directly. The number of OIG fraud referrals our frontline employees took about allegations of Social Security scam calls jumped from just over 5,000 allegations in FY 2018 to more than 60,000 in FY 2019. We estimate the call volume to our 800 number related to phone scams to be over 850,000 last fiscal year. As I visited SSA field offices and teleservice centers, employees told me their firsthand accounts of

[1]The Do Not Originate (DNO) process permits telephone companies to terminate spoofing calls across their networks. As of September 16, 2019, 100 percent of our published toll-free telephone numbers have been processed by major US telecommunications providers.

how these scam calls affect Americans and our frontline service. I made working with SSA's IG Gail Ennis to combat these fraudsters a priority.

We have:

- Created a dedicated online scam form to allow OIG to collect the data it needs to investigate, identify, and stop scammers and produced new television and radio public service announcements promoting the new form;
- Improved the OIG Fraud Hotline and our 800 number to provide information to callers about the scams and how to report them online;
- Increased employee and public outreach and education; and
- Established an SSA and SSA/OIG workgroup to ensure we are providing the kind of expertise and attention that can timely identify and implement improvements and find additional ways to curb scammers.

Online Scam Form

Often our frontline employees in the field or on the 800 number are the first to hear from the public about impersonation scams. Thus, these employees obtain information needed to investigate these scams; however, SSA and OIG have distinct responsibilities. SSA's role is to identify and remedy potential service problems associated with the scams, and of critical importance, to educate the public. OIG's role is to collect and analyze reported information, identify leads that could help root out these criminals, and support their prosecution.

To help ensure swift action against these criminals, OIG needs to quickly receive scam reports and obtain the data it needs. A dedicated scam reporting form is a best practice identified by Treasury Inspector General for Tax Administration in handling Internal Revenue Service imposter complaints, which have sharply declined while the SSA scams have skyrocketed. In November 2019—about a month after we established our SSA-OIG workgroup—we implemented a dedicated online scam form that allows people to report to our OIG Social Security-related scams, including robocalls, live calls, email, text, and in-person scams. The OIG uses the online form to capture the data it needs to analyze trends, identify investigative leads, and identify criminal entities and people participating in or facilitating the scams. The form also requires individuals to create a unique Personal Identification Number, so if the OIG contacts them, they will know the call is legitimate. In addition to helping the OIG collect the data it needs, the form alleviates some traffic and wait times in our frontline offices. So far, our OIG has received over 115,000 submissions.

We will continue to support this effort and work with OIG to implement changes to the fraud reporting form as needed to respond to evolving fraud trends.

Improvements to 800 Number and Fraud Hotline

To help OIG collect the data it needs to stop scammers, we added a message to our 800 number recordings directing callers to report online. All English and Spanish-speaking callers to our 800 number and field offices now hear the following message: "We have received reports about

fraudulent phone calls from individuals impersonating SSA employees. If you suspect you have received a scam call, you should report the details of the call to the Social Security Administration's Office of the Inspector General online at oig.ssa.gov."

We also helped the OIG update the Fraud Hotline message to provide scamming information upfront and to direct Hotline callers to the online form. The changes to 800 number and Fraud Hotline are having measurable effects. Transfers from the Fraud Hotline to the 800 number are down significantly, and I understand fewer callers are requesting to speak to a representative on the Fraud Hotline.

Outreach and Education

In our ongoing fight against fraudsters, one of the most powerful tools is public education. We have armed our frontline employees with instructions and updates on how to assist potential victims of phone scams, and we are communicating scam information agency-wide. We are also redoubling our public education efforts and raising awareness in as many ways as we can think of, starting with new public service announcements that are being distributed across the country. Our increased focus on scams and collaboration with OIG is also helping us notify employees and the public timely as scams evolve. Earlier this month, we shared information from OIG about new twists that involve spoofed emails purporting to be from us.

We appreciate your help, too. Last month, we provided material to Congress with a request that you help spread the word to your constituents through your powerful communication tools—town halls, local print outlets, television, and social media. I highly recommend using these materials to inform your constituents. We all share responsibility to fight this serious threat to those we serve. We also invite you to share ideas of what else we can do.

We are working now to arrange radio campaigns on nationally syndicated talk shows and television appearances on popular morning shows. We are also expanding our work with external groups and agencies like AARP and other organizations representing seniors, representative payee organizations, motor vehicle administrations, the United States Postal Service, and the Department of Veterans Affairs. I recently met with AARP's Chief Executive Officer JoAnn Jenkins, and we are working on a joint public service announcement. AARP has also agreed to promote our scam prevention messaging on their social media channels.

As we conduct our public awareness campaign, we will continue to collaborate with OIG, the Federal Trade Commission (FTC) and others to curb scams and respond quickly as scams continue to evolve.

Broader Solutions

I want to close by reiterating that we are eager to end these phone scams, but understand that scammers may simply move to target another agency as we and OIG work to shut them down. We need broad solutions, and I want to thank Congress and the President for recently enacting the *Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act*, or

Pallone-Thune TRACED Act (Public Law 116-105), which will help the Federal Communications Commission prevent scam calls from reaching the public.

Conclusion

I want to thank the FTC for its ongoing support, advice and actions. I also thank our IG for collaborating with me on this priority. I do appreciate that this effort requires resources.

Scammers are sophisticated. We want everyone to know that if they get a suspicious Social Security-related call, hang up and report it at oig.ssa.gov. Do not trust caller ID, do not give your Social Security Number or other personal information. Do not provide money. Our employees will never threaten or demand money from you.

I thank this Committee for holding this hearing to elevate the visibility of these scams. I appreciate your interest in this important issue and look forward to working with our OIG and other partners like the FTC and Congress to protect Americans. I would be happy to answer any questions.

United States Senate

Special Committee on Aging

Statement for the Record

That's Not the Government Calling: Protecting Seniors from the Social Security Impersonation Scam

Gail S. Ennis

Inspector General
Social Security Administration

January 29, 2020

Chairman Collins, Ranking Member Casey, and Members of the Committee:

Thank you for inviting me to testify today. I am pleased to be here to discuss the efforts of my office to raise public awareness of Social Security telephone scams and to disrupt the scams.

Introduction and Overview

For the better part of a decade, Americans' landlines and mobile phones have been plagued by widespread robocalls and live callers impersonating government agencies to mislead victims into giving them personal information or money. In the fall of 2018, the Social Security Office of the Inspector General (OIG) saw a spike in complaints about callers impersonating Social Security employees or alleging a Social Security number problem. As an indication of the severity of this spike, in fiscal year (FY) 2018, we recorded about 15,000 of these scam complaints; in FY 2019, we recorded over 478,000 (see Exhibit 1 for month-over-month complaint totals).

Today, Social Security-related phone scams are the most common type of government imposter scam reported to the Federal Trade Commission (FTC). As a Wall Street Journal headline recently articulated, Social Security scams "exist because they work." Scammers may "spoof" legitimate government numbers so those numbers appear on caller ID, and in the latest variants of the scam, they may tell victims about a fine or debt they need to pay to avoid arrest or other legal action, resolve a Social Security number problem, or increase a benefit. They demand payment using cash, retail gift cards or pre-paid debit cards, wire transfers, or internet currency, all of which are difficult to trace. They may quickly escalate threats to frighten victims into complying, and have emailed fake letters and reports that appear to come from Social Security or its OIG, to convince potential victims of their legitimacy.

Social Security phone scams are widespread across the country and reach people of all ages. Of our FY 2019 complaints where the complainant provided a date of birth, the median age was 59 years old. The median age for the United States was 38 years old, but we cannot draw conclusions about why our complainants tended to be older than the population at large. The FTC recently reported that younger people fall victim to government imposter phone scams at higher rates than older people, but the latter group reports higher fraud losses when they do fall victim. For example, about 81 per 100,000 people ages 20-29 years old reported a fraud loss to the FTC due to government imposter scams in FY 2019; for those ages 80 years or older, the rate was about 40 per 100,000. However, the median fraud loss amount for those ages 20-29 was $1,000, while for ages 80 and over, it was $3,000.[1]

We recorded scam complaints in FY 2019 from people residing in all 50 States, Washington, D.C., and several U.S. territories, more or less in proportion to the population of each jurisdiction. Only about 1 percent of complainants reported having lost money to a Social Security phone scam.

Nevertheless, these scams have a significant and detrimental impact on the public and on Social Security's ability to administer its programs. First, they have caused and continue to cause untold anguish and financial harm to the those who fall victim to scammers' sophisticated tactics, sometimes losing sums in the hundreds of thousands of dollars. The scams have also caused a strain on agency and OIG resources. SSA needs to be able to disseminate accurate and timely

[1] FTC Interactive Data Dashboards, https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2019.

information to millions of individuals, and the volume of scam-related complaints has made this more difficult. On the OIG side, our fraud hotline volume increased ten-fold in one year, increasing our costs and straining our ability to answer calls. Finally, the scam erodes the public's trust in Social Security, and in government overall. For example, our investigators now have encountered witnesses who did not believe they were Federal agents and would not speak to them, making it more difficult for us to conduct legitimate fraud investigations.

For these reasons, we know SSA and my office both must act to educate the public about scams that use the name of Social Security to defraud, and combat the scams themselves. Soon after I was sworn in as Inspector General last year, I directed my staff to undertake a multidisciplinary approach to this issue. We are:

- raising public awareness through online messaging, publications, and news coverage, and engaging in an outreach campaign to public and private partners to collaborate on ways we can reach even more people with our educational message;

- responding to congressional requests for information that will help inform the government's response going forward, including evaluating SSA's efforts to address the scams; and

- devoting significant resources to investigative efforts, working in concert with the Department of Justice and other law enforcement agencies, and leveraging technology to create a dedicated online reporting form that reduces processing time and allows us to collect targeted data to generate leads for investigative and disruption efforts.

We are working on all these fronts to reduce the number of people who fall victim to these pervasive and insidious scams.

Raising Public Awareness

Without question, short of completely eliminating telephone scams, the most effective way to combat them is by educating the public about this phenomenon and how people can identify and report scam calls. The OIG is a small agency of approximately 540 employees, with limited resources with which to conduct public outreach on any issue, including Social Security scams. Therefore, to scale our outreach efforts and expand our reach, we have partnered with SSA, FTC, the American Association of Retired Persons (AARP), and others to raise public awareness about Social Security scams.

Scam Awareness and Reporting Messaging

First, we have redesigned our website home page so people can easily understand how to report Social Security scams to us as well as other types of Social Security fraud. We also redesigned our "Scam Awareness" webpage with links to FTC scam resources and SSA's new public service announcement and flyer, and we will continue to add resources and links to that page so the public and advocate agencies can find what they need to assist people in local communities. And, we shortened the website address for easy access: https://oig.ssa.gov/scam.

We are regularly consulting with SSA to ensure the agency's messaging is consistent and up to date on current scam trends. We are currently working with SSA and the U.S. Postal Inspection

Service (USPIS) to co-brand an SSA scam warning poster with the USPIS logo and mail fraud-related warnings. USPIS then plans to put the co-branded poster (or corresponding digital signage) in U.S. post offices across the country, reaching potentially millions of people. We are also planning a "National Slam the Scam Day" campaign, designating a day to educate the public and promote government imposter scam awareness. We hope to engage Federal agencies, the IG community, Members of Congress, private-sector companies, and elder care advocates in unified support of this campaign. We plan to use news coverage, social media and website outreach, and live events to reach Americans with our key scam awareness messages.

Finally, we have streamlined our fraud hotline messaging to include scam awareness information, and to encourage callers to use our new dedicated online scam reporting form. The new messaging has resulted in the number of scam-related calls to our hotline dropping to historically normal levels; our hotline personnel are now answering nearly 100 percent of calls. To accompany these changes, we implemented design changes on our website so that visitors are easily able to find the scam reporting form, linked directly from our home page. We are also currently developing a paper version of the online form that the public will be able to mail or fax to our fraud hotline for processing. These modifications are improving the efficiency and effectiveness of the information collected from complainants.

Media Outreach

We are continuing our efforts to increase coverage from the media about Social Security scams, including our new online reporting form, and new scam developments as they occur. After we issued a joint press release by the Inspector General and the Commissioner of Social Security announcing the dedicated online scam reporting form, we saw significant related news coverage, including by Forbes, The Washington Post, and the Associated Press—and we continue to see news coverage daily. Due to this publicity, as of January 18, 2020—barely 10 weeks after launch—we had received over 111,000 complaints through the new online form.

We also update our public messaging quickly as the scams evolve. Recently, we received information that scammers were emailing fake letters and reports using SSA and SSA OIG letterhead images, to convince victims of their legitimacy. We redacted those fake documents and made them available on our website as well as to multiple media outlets that requested them, to spread awareness as quickly as possible. In recent weeks, we have also given interviews to AARP and Cox Media Group, the latter for a scam segment that aired on local television stations in major metropolitan areas. This week, we have a spokesperson appearing on a New Mexico TV and radio show that reaches 99 percent of that state. Next week, we will participate in an AARP tele-town hall event in Maryland, speaking about scam awareness. We will continue to work with the media to the greatest extent possible, to disseminate our key messages and educate the public.

Collaborative Outreach Campaign

In August 2019, we began an outreach campaign to other agencies, search engine and social media companies, nonprofit agencies, and corporate retail entities to collaborate on raising public awareness, and ask for suggestions and best practices. For example, we have met with the FTC, the Consumer Financial Protection Bureau, and Elder Justice Coordinating Council Working Group members at various agencies. We have talked to Google and Microsoft about ways they may be able to use their search engines to warn people about scams. We have also sought

guidance from Twitter on how to expand our reach on their social media platform, using hashtags to become "trending" and using that as a method to spark both public conversation and media coverage of the scams.

With regard to nonprofit agencies, we have joined forces with SSA to ask AARP to host a government imposter scam awareness webinar. An AARP webinar would be available to the organization's 38 million members, providing valuable fraud prevention information to senior citizens and the elder care services community. In addition, the Downtown Baltimore Partnership has disseminated our scam information to its city resident mailing list of 15,000 members, its membership network of 650 companies, and its network of sister organizations across the country. We also met with the National Retail Federation (NRF), the world's largest retail trade association. They plan to send Social Security scam information to their members, and they connected us to a gift card marketer that subsequently agreed to include information about Social Security phone scams in anti-fraud training they provide to retailers on gift card fraud.

We reached out to corporate retailers including Wal-Mart, Target, Walgreens, and others, to discuss approaches for point-of-sale consumer education that might help prevent scam victims from following through on gift card purchases. As part of this retailer outreach effort, we worked with SSA to create a sign that retailers could place on gift card kiosks to warn the public about scams at the point of sale. Wal-Mart has added this sign to its rotation of anti-fraud messages showing on large video screens near the customer service desk in 2,100 U.S. stores; they will expand this effort as they renovate stores to include the video screens. In addition, Amazon has placed a Social Security scam warning at the top of its "Be Informed" gift card fraud page. For entities that we have not been able to reach, I recently sent a letter inviting them to collaborate with us to protect their customers from fraud. We will continue to follow up as well as reach out to new organizations to raise public awareness.

OIG Audit and Investigative Efforts

Audit Work

On December 23, 2019, we responded to your Committee's letter asking for information about SSA's and SSA OIG's efforts to combat these scams and educate the public. In our response, we explained OIG's investigative approach and communication and outreach strategies. To respond adequately to your questions about SSA's efforts—and to answer similar questions from the House Committee on Ways and Means, Subcommittee on Social Security—our Office of Audit has initiated a formal review of SSA's efforts to combat the scams, and how the scams have affected the agency's operations. As of January 24, 2020, we are awaiting SSA's response to our auditors' questions. We anticipate that our Congressional Response Report with this information will be issued by the end of March 2020, and we will be able to provide more information about SSA's efforts at that time.

Investigative and Disruption Efforts

In April 2017, soon after we first identified an upward trend in allegations related to Social Security phone scams, we created a National Operation Code in our investigative management system to track and monitor complaints. We also began communicating with other similarly affected OIGs and the FTC to share best practices and other information, as appropriate. In

particular, our Office of Investigations reached out to the Treasury Inspector General for Tax Administration (TIGTA) to learn how that office had addressed IRS phone scams, as they had been widespread since 2013.

In the spring of 2019, we reassigned investigative personnel to OIG headquarters to centralize investigative efforts to combat the scams. This fall, we reorganized those personnel into a new division, the OIG Major Case Unit. This structure allows the Office of Investigations to focus investigative, analytical, and legal resources to combat the scams, which have a national and multi-jurisdictional scope and breadth. The Major Case Unit is coordinating investigative efforts among OIG offices throughout the United States, and across jurisdictional lines and with other law enforcement agencies. The unit is also liaising with private-sector entities to leverage available resources. These partnerships act as a force multiplier, giving us resources throughout the country to investigate and disrupt ongoing imposter scam activity.

We have implemented a three-tiered approach for our investigative efforts: top-down, bottom-up, and disruption. Top-down refers to our investigations into the scam calls themselves and those entities and individuals who facilitate them. We are conducting these investigations in close coordination with the Department of Justice, including its Transnational Elder Fraud Strike Force. As our investigations are active and ongoing, we cannot share further details at this time. However, we will provide information as we are able to do so.

Bottom-up refers to targeting the "money mule" networks that collect, launder, and move money received from victims. On December 4, 2019, the Department of Justice announced a money-mule enforcement initiative by a coalition of law enforcement partners, including SSA OIG. We have several ongoing investigations working jointly with Federal, state, and local law enforcement partners, including USPIS, TIGTA, United States Secret Service, Department of Homeland Security's Homeland Security Investigations, and others. Again, we are unable to provide specific investigative details at this time, but we can provide a briefing at a future date when we can say more.

Disruption refers to our collaborative efforts with SSA and the U.S. telecom industry to impair the ability of robocallers to "spoof" SSA phone numbers on caller ID to deceive people, and to shut down telephone numbers used by the scammers. Last year we initiated a "Do Not Originate" process with Verizon, and with assistance from SSA we can now report that all major U.S. telecoms have implemented 100% blocks on spoofing publicly available SSA field office phone numbers. These efforts have blocked millions of spoofed calls, making it harder for the scammers to fool the public into thinking the scam calls are coming from SSA. We continue to work to add SSA telephone numbers to DNO lists as it becomes necessary. We have now implemented a second phase of disruption, where we request that telecom companies suspend or terminate phone numbers that are reported to us as being call-back numbers for Social Security scams.

The most important step we have taken to manage our scam-related workload—and to develop actionable investigative leads—has been implementing a dedicated online reporting form. This was a best practice identified by TIGTA in handling IRS imposter complaints. We worked with SSA systems personnel to develop the form and link it from the OIG website. The dedicated online form went live on November 16, 2019, and we immediately saw benefits: we are receiving complaints more timely from the public, with more targeted information, including scammer call-back numbers, caller ID numbers, and fraud loss amounts, in a format that is easy

to track and analyze for investigative leads.

Scam-Related Challenges

As you can see, we are working on multiple fronts to combat Social Security scams and reduce their impact on the American public. Unfortunately, the scams and the scammers continue to evolve, and we expect they will soon move on to new tactics and techniques. We will continue to face an ongoing challenge of limited resources with which to combat Social Security phone scams and raise public awareness of them. One way of addressing this challenge would be to authorize asset forfeiture, allowing law enforcement agencies to seize funds involved in, and assets gained from, fraud schemes. Agencies could then use those funds for initiatives such as a victim restitution fund or consumer protection outreach.

The broader challenge facing the Federal Government, however, is that this is not just a Social Security problem. Just two years ago, IRS scams were the headline. Next month, it could be Veterans Affairs, Homeland Security, or the Census Bureau. This is not even just a government agency problem. On the FTC's Scams page, you can read about family emergency scams, real estate investment scams, tech support scams—even romance scams. It is clear the Federal Government must work collaboratively to combat robocalls and telephone scams of all kinds.

We thank you for your efforts to date to find legislative solutions that can comprehensively address this complicated issue. We appreciate the recent enactment of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, Public Law 116-105, which is a step forward in protecting the public from scam calls.

We are aware of legislation proposed by Committee Members, such as S. 2147, the Anti-Spoofing Penalties Modernization Act of 2019, which doubles the penalties for providing inaccurate caller identification information and extends the statute of limitations for penalizing persons who commit such violations. Additionally, S. 149, the Stop Senior Scams Act, establishes a Senior Scams Prevention Advisory Group, which would create model educational materials to educate employees of retailers, financial-services companies, and wire-transfer companies on how to identify and prevent scams that affect seniors.

We are also aware of bills that Committee Members support, such as S. 512, the Seniors Fraud Prevention Act of 2019, which directs the FTC to establish an office within the Bureau of Consumer Protection to advise the FTC on the prevention of fraud targeting seniors and to assist the FTC in monitoring the market for mail, television, Internet, telemarketing, and robocall fraud targeting seniors. Your efforts show a commitment to combat this fraud, and we are available to work with your staffs on these or any other proposed bills. We encourage Congress to further assist us by continuing to pursue legislative solutions that will hold accountable U.S.-based telecommunications companies that introduce scam call phone traffic, including from overseas, into the U.S. telephone system.

Finally, we have recently identified a distressing problem surfacing among those who fall victim to Social Security phone scams and lose money to scammers. Those who empty their retirement accounts to pay scammers may face harsh tax penalties for doing so before they reach the minimum withdrawal age. We understand the solution to this problem may not be easy, not least because it may be difficult for scam victims to provide proof of their own victimization so they can become eligible for any relief that could be made available to them. However, we encourage Congress and

the agencies involved to be aware of this issue, and explore ways to avoid victimizing these individuals twice and help ameliorate the losses they have suffered.

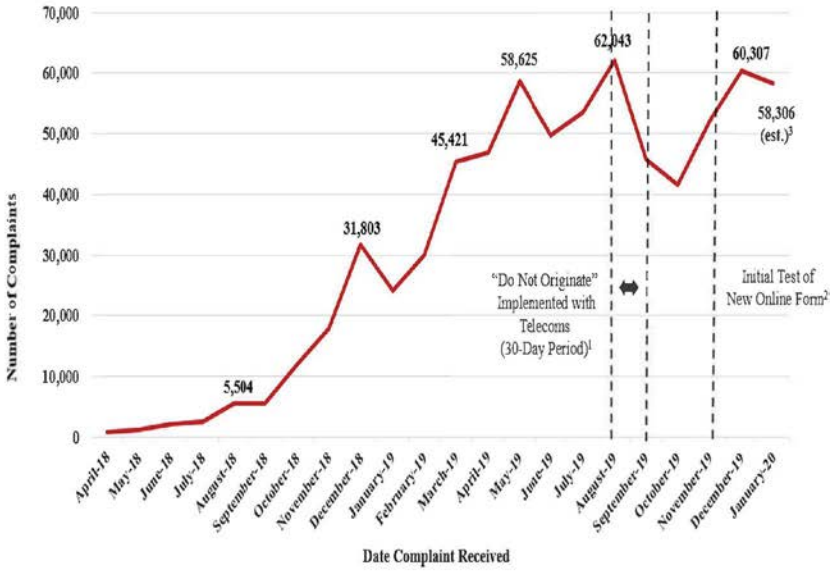
Conclusion

We have dedicated significant resources to combating Social Security phone scams, and we have seen positive results from our efforts. We hope, as we and SSA reach more people, they will have the knowledge to be able to avoid becoming victims, and they will report scams to us, giving us more valuable data to work with for investigative leads and outreach targeting. From our experiences, we stand ready to assist the next government agency that may become the target of imposters, and we look forward to sharing our best practices with them.

Thank you for holding this hearing today to discuss ways to protect our citizens from these scams. These scammers have robbed too many people of their hard-earned savings, and we must continue to leverage resources across agencies, and use innovative approaches to stop the scams and protect Americans. Your involvement and interest spurs increased attention to the issue, and helps move us closer to a comprehensive solution. Thank you again for the invitation to testify, and I am happy to answer any questions.

Exhibit 1

Impersonation Scam Complaints Received by SSA OIG (April 2018 to January 2020)



Note 1: We secured partnerships with major telecoms in August and September to initiate "Do Not Originate" efforts.
Note 2: While the press release on the new online form was issued November 19th, testing of the form began November 16th.
Note 3: The January 2020 estimated complaints figure was calculated using data through January 18, 2020.

Testimony of Machel Andersen

Before the
Special Committee on Aging
United States Senate

January 29, 2020

Chairman Collins, Ranking Member Casey, and Distinguished Members of the Committee; thank you for the opportunity to appear before you today to tell you how international criminals used the Social Security scam to steal $150,000 from me and my husband, money we had worked our entire lives to save.

This terrible story began less than two months ago, on Friday, December 6. I was a little bit busy and distracted that day, because one of my daughters had just had surgery and needed help and I stepped in to watch the grandkids. At some point, I noticed that I had missed three automated voicemails from what appeared to be the Social Security Administration, with messages telling me that my social security number had been "compromised." When I called the number in the voicemail back, a man who claimed to be "Joseph Gangloff" answered. He told me he was with the Social Security Administration, he gave me his badge number, and he told me that if I looked him up online, I would find that he was the Chief Counsel to the Social Security Administration.

Then he told me some bad news – my Social Security number had been compromised and a car registered in my name was found with blood all over it at a crime scene near the Mexican border. He asked me if I had recently been to Texas? I assured him I had never been to Texas.

Worse, he told me that my social security number had been used to set up multiple bank accounts associated with a drug cartel, and he then transferred me to someone who claimed to be a DEA investigator named "Uttam Dhillon." This man told me that my family was in danger, that my social security number was being used by a very powerful drug cartel, and that they would be watching my every move. He told me that the only way to ensure that my family and I would be safe was to cooperate with the government who would also be watching me. He told me that any accounts I had associated with my social security number would be seized as part of the DEA investigation, and that I needed to cooperate by transferring all of the money in all of my bank accounts to an off-shore account that would be safe, before the fraudulent accounts were seized, or I would lose all of our money. He told me that he would be watching my bank account, and that if I made any kind of withdrawal, they would know. Also, if I didn't cooperate, I could be suspected of working with the cartel.

But he promised that if I did what he asked, he would "protect" my family and I, and I would get all my money back later, along with a new social security number.

I thought it was a little strange that this man had an Indian accent, but I looked him up on the DEA web site, and it turns out that Uttam Dhillon really does work for the DEA, and appeared to be of Indian descent.

Next, this scammer told me that I need to get in my car and calmly and carefully drive to every institution where we had money that would be connected to my social security number, withdraw it and put it in one account where I would then need to wire transfer it to this "safe place". I got so upset by all of this that I began to cry. He told me "no crying."
He insisted that I needed to, "act normal and happy," and not tell anyone, this was very important – and he reminded me that the bad guys were watching everything I was doing and the government was too. It was late and I was very upset. I told him I couldn't get to every financial institution where we had money before they closed. He told me to go to the one that had the largest amount first. He told me to transfer everything into my checking account. He said that he wanted to be on the phone while I made the transfers and that I was then to come back to my car where he would give me the information to wire transfer the funds. He told me that I would need to tell the teller that I was buying "electronics." I told him I didn't lie. He said that he understood, but that this was for the "greater good".

By the time I arrived at the credit union, it was about 5:50 pm, too late in the day to send transfers overseas. But I was able to transfers all of my money out of our savings accounts, including closing all our CD's and incurring penalties, into our checking account so it would be ready to send first thing Monday morning. I got in my car and started for home. He asked me to pull over where I could safely fulfill the rest of the requirements to ensure my safety. He asked for my email address and said he was sending me an official warrant for my arrest. When it came he asked me to look it over carefully. I did so. It looked official but I have no experience in these matters. He asked me to locate a piece of paper and write what he told me to write and send a picture of it along with a picture of my driver's license to him. He asked me to write that I would cooperate fully with the government and that in the case that I didn't, I understood that it would mean my immediate arrest and possible harm to my family. I was again reminded that under no circumstance was I to mention this to anyone. He brought the supposed Joseph Gangloff back on the line and they asked me to cooperate as they connected my line with theirs as a way to monitor my movements. I was to say hello every 5 seconds until this process was complete.

That weekend was very tough. I decided to call the scammer back to see if there was some other way to handle the situation. He said that I had the choice to be arrested immediately and that I did not have to cooperate with him. I told him I would like to Facetime him in order to make sure he was who he said he was. He said that was not possible. I asked for him to send

my local Sheriff to my door to confirm that this was a true story. He said that he would do this on Monday morning. Unfortunately, Monday morning when he called to ask if I wanted the Sheriff to come to my door, I was 50 miles away caring for my daughter and grandchildren, and not able to meet with the Sheriff.

I told him I would just have to trust him. I dropped my granddaughter off at school and drove to Golden West Credit Union where I had a certificate of deposit, and cashed it out, paid the penalty, and took the cash to the closest American First Credit Union, to make the wire transfer. He sent me the information for the account I was to transfer the money to by text. The scammer insisted that I keep him on the phone with me the entire time that I was in the credit union. I put the call on speakerphone, and put the phone in my purse. He reminded me I would get all the money back when this was over, and told me I could hold back $1000.

I had my 7-month-old grandson with me in a car seat and had to haul him into the credit unions with me to do these transactions.

When the teller asked what the money was being used for, I said that it was for "electronics", just like the scammer told me. That was the only question I was asked.

I sent the money to the Bank of China in Hong Kong -- $118,464.00.

I sometimes wonder what I might have done if someone had asked me more questions. But the scammers had me so worked up – they told me that I had to be convincing or I would end up getting arrested and my family could be hurt. I completed the wire transfers much easier than I had anticipated. I was afraid that they may not let me make the transfer. I was told to take pictures of the receipt and send it to him so that he could have proof that I truly had made the transfer. He in return sent me a verification from "Berkshire Hathaway" certifying that they had received the money and that it was being safely held until I was issued a new social security number.

The scammer made contact several times a day either by call or text to keep me updated on the progress being made on the case. Wednesday morning he called to ask if I was certain I had everything accounted for as I would for sure lose anything that wasn't secured. I was panic stricken as I remembered that I was joint owner on my mother's account and possibly some of our children's accounts. I told him we had some investments, but that we had recently cashed what we could out as we had plans to invest that money in some other stocks. He told me to find out what accounts I was joint on and as best I could without letting them know that I was working with the Social Security Administration and the DEA and let him know roughly what the balances were. I did, and he was able to get "special permission" from the Supreme Court to waive these accounts. He asked where the investment funds were and I told him they were safely in a check on my desk. He told me that the check would have been drawn on an account

linked to my social security number and needed to be deposited also to protect it. I drove to the credit union and deposited a check for 35,000.00 into my account. He said I would then have to come back to my car to get the wire transfer information. He advised me to go to another branch to eliminate suspicion when making the wire transfer and I did.

The next day the scammer asked me about the value of our home. I told him we owned our home outright – if was fully paid off. He told me that I needed to get a mortgage and pay 45 percent of the value of the house to him right away – about $200,000 in order to secure my home as it was also connected to my social security number! I asked how my house could be connected to my social security number with no mortgage? He told me all of our assets whatever they might be were connected to my social security number. I told him that I couldn't get a mortgage on the house without telling my husband, and I just wasn't going to do this – he threatened to have me arrested, and I told him that he could go ahead and send the Sheriff, I was not going to get a mortgage on my house.

He told me to start approaching friends and see if I could borrow the money for a few days.

I approached a close friend who I thought might have that kind of money, and he told me he could get me $60,000 right away, and the rest of the money in a couple of days. He asked me if I was being scammed? I assured him I was not, and that I would get the money back to him most likely in the middle of the next week.

I almost went through with that. I was able to leave my daughter's home and spend the afternoon cleaning my home and getting ready for the weekend. As I was cleaning, I felt impressed to check again online to see if this was for real. So, I searched Google, and found out pretty quickly it was all a scam. I was devastated.

My husband and I had plans to meet some friends for dinner and a concert in Salt Lake that night. I didn't want to ruin the evening for my husband, so I determined that I would tell him on our drive home. It was a very hard thing to tell him that I had lost all of our savings. He was so kind and understanding.

For the last six weeks I have been asking myself how this could ever have happened to me? My husband and I had worked hard all our lives to save the money the scammers stole from us. We had hoped we could travel, and do mission work, with the money we had saved. Now, we can't. Instead, we will need to work to try to replenish what I lost.

I don't know if I will ever stop wondering why this happened. Having our life savings stolen has made me realize that there are some very bad people in this world. But losing this money has also reminded me that my life is rich in ways far greater than stolen money. I live a wonderful life, in a wonderful place. I have a great husband, and a great family. I am truly blessed. Maybe

hearing my story will help protect someone else, and some other family that would have a harder time recovering. Or maybe the government could take action to require financial institutions to provide more information and ask more questions before making international wire transfers from a non-business account. Maybe my story will help stop these scammers, once and for all.

I hope so.

Thank you for allowing me to tell my story here today.

United States Senate Special Committee on Aging

Testimony of Justin Groshon
New England Social Security Management Association (NESSMA) President

National Council of Social Security Management Associations (NCSSMA)

Hearing on "That's Not the Government Calling: Protecting Seniors from the Social Security Impersonation Scam"

January 29, 2020

Chairman Collins, Ranking Member Casey and Members of the Committee, my name is Justin Groshon. In addition to being president of the New England Social Security Management Association and a member of the National Council of Social Security Management Associations' executive committee, I am the District Manager of the Saco, Maine, Social Security office. On behalf of the National Council, thank you for the opportunity to be here today and to submit this testimony regarding Social Security impersonation scams.

The National Council of Social Security Management Associations is a membership organization of over 3,100 Social Security managers and supervisors, in the agency's 10 regions, who provide front-line leadership in over 1,200 field offices and teleservice centers in communities across the country. Since the founding of our organization fifty years ago, we have supported the agency in building trust among the American people. This includes not only the payments we issue each month to tens of millions of people, but also the trust that Social Security will protect their most personal information. Our organization firmly believes that these impersonation scams erode the trust the public has in our agency.

As New England president, I represent over 180 managers and supervisors in the Boston Region, including 22 in the State of Maine. Despite agency employees' best efforts to reassure the public and help them protect their information, the number of impersonation scams in Maine and across the country has been on the rise over the last year.

In October 2019, the National Council conducted a survey on various scams and the impact on Social Security field offices and teleservice centers nationwide. We received responses from over 500 managers and supervisors on the impact to their respective offices. Over **97%** responded that their office received reports of someone calling a member of the public and impersonating a Social Security employee. Of those, almost 70% reported that this was a daily occurrence with 50% reporting as many as 15 contacts per day.

In my home State of Maine, every field office has been impacted by a wide variety of scams. Every day, our offices receive calls from the public reporting Social Security

impersonation scams. Every office in Maine has experienced the fallout and lasting influences of calls impersonating Social Security employees.

Social Security field offices in Maine served almost 300,000 customers in Fiscal Year (FY) 2019. Each day, almost 500 residents of Maine visit a Social Security office. Every office in Maine has received calls and visitors reporting that people are impersonating Social Security employees. To exacerbate the problem, fraudsters have "spoofed" or masked their own telephone number with that of a field office's general inquiry telephone number in an attempt to trick the public into thinking they are receiving a legitimate call from a Social Security office and representative. Consistent with press releases from the Social Security Administration's Office of the Inspector General, the people of Maine and all across the country receive threats of legal action, fines, arrest, or promised increases in benefits in exchange for the payment of fees.

For many, these calls understandably result in fear and anger. A significant number of customers call our offices in an attempt to verify the authenticity of the threat. In some instances, calls to Maine offices increased by 400 to 1000%! The public questions the legitimacy of the call they just received or a voicemail they listened to, and callers from all across the country and some from overseas begin contacting a single field office for assistance. The increased call volumes prevent the agency from being able to conduct business with those seeking our core services.

Further complicating these scams, many fraudsters use Social Security telephone numbers to set up automated calls and messages. This results in field offices receiving hundreds of unsolicited calls each day. To illustrate, an office in Maine received more than four times their average number of calls over a 22-day period. One day alone they received 1,930 automated calls to the office general inquiry line. These calls prevented members of the public from receiving our help and ultimately, that office went through the process of changing their telephone number. The increased calls to offices resulting from these schemes can last several days and even weeks.

In addition to higher call volumes, there is a new stream of visitor traffic to report the schemes. In every Maine office, employees have reported greater numbers of customer complaints from visitors expressing concern because they disclosed their personal information to the fraudsters believing they were receiving legitimate phone calls. Our callers and visitors are scared, upset and confused. They are concerned about their personal information and the level of sophistication used by the scammers.

In addition, online processes and applications put in place to provide additional service options, which often reduce the number of telephone calls and field office visitors, are compromised as the public places less trust in these services. Customers are understandably leery of Social Security's online services and are reluctant to use them, driving more people into field offices in order to confirm they are transacting business with a legitimate representative.

As part of the National Council survey, Social Security field office and teleservice center managers and supervisors provided their anecdotal feedback based on contacts with customers regarding these impersonation scams. The following feedback further illustrates the impact on Maine field offices.

- Field offices experience an increased rate of abandoned telephone calls because customers have to wait longer to receive an answer. This leads to more members of the public walking into field offices for services they could otherwise receive over the telephone. This only exacerbates the problem for those offices that also experience spoofing of their general inquiry line.

- Impersonation calls have eroded the public's trust. Even with scheduled appointments when a member of the public is expecting a call, they are often skeptical of our identity. Often, they refuse to speak with an actual Social Security employee because they are suspicious of the calls. This has had a significant impact on many workloads and has slowed down production, resulting in frustration for the public and Social Security employees alike.

- Members of the public contacting offices regarding these scams are taking precious time away from serving other customers who are seeking benefits, payment changes, or other core services. These scams place additional demands on office and employee resources, detracting from our agency's mission.

- There is an overall sense of panic, especially for those who disclosed personal information to scammers. They think Social Security has the ability to do more to protect their personal information. Unfortunately, this is often not the case.

- The American public incorrectly believes we have a system to add fraud alerts to their record or that we can do something beyond routing their fraud allegation and giving them the Federal Trade Commission ID theft publication. Police departments send members of the public to Social Security, believing we have some type of system to address the scam calls and record the incident. Clients feel ordered by law enforcement to come in and "file a report" and are often upset when they wait for service and then learn we cannot add a fraud alert to their record.

- The scam calls have the most impact on the elderly. These individuals frequently require face-to-face interviews to explain and reassure them that their account information has not been compromised. Family members often call on behalf of the elderly and enter into tense discussions involving disclosure of information issues because we are unable to disclose any information to a third party without consent.

- Victims report that scammers tell them that their Social Security Number (SSN) has been linked with a crime and that the scammer needs information and/or payment to prevent their SSN from being suspended. Reports also detail how

members of the public are threatened with arrest or being reported to law enforcement if they do not respond.

- Some victims who have fallen for the scam have complied with instructions to purchase pre-paid debit cards, Google Pay, or other gift cards. The scammer then calls the victim back to obtain necessary information from the cards to be able to liquidate the funds.

In my own office, the general inquiry telephone line, the number I rely on to serve the public, was used in an automated call scam. This scam occurred on three separate occasions lasting three days each. This significantly reduced our ability to serve the public, degrading service to not only the residents of Saco, but to everyone my office serves.

These rampant fraud schemes are not isolated to Maine. My colleagues from all 50 states have experienced similar issues. On any given day, offices across the nation see 172,000 people and field more than 445,000 telephone calls. These additional visits and calls regarding these scams impede our agency's ability to serve the public, increasing wait times and decreasing telephone answer rates. Based on our National Council survey, 43% of respondents reported that between 3 and 10 customers visit their office every day to report an impersonation fraud scheme. Over 10% reported as many as 10 to 25 additional visitors each day. A majority of survey respondents, 70%, also reported that the impersonation schemes have affected their ability to answer telephone calls. In addition to higher call volumes, employees are spending more time with each caller in an attempt to alleviate fears and restore faith in our agency. To put this in perspective, we estimate that over 2 million people will contact Social Security this year to report a fraud scheme. If employees spent 8 minutes with each customer, who had been a victim of an impersonation scheme, we estimate the agency would need to devote 130 full-time employees, each year, to just this task.

Based on survey feedback, many offices across the nation have expressed the same concerns as those expressed by managers in Maine field offices. It is important to note the additional feedback managers provided across the country.

- Employees conducting legitimate Social Security business are met with suspicion, leading to repeated telephone calls, the need for members of the public to visit the office, and delays in processing claims or other post-entitlement work.

- Field offices with increased telephone traffic, due to the impersonation scams, have been forced to redirect resources from serving those walking into our offices to telephones. This results in additional employees taken away from processing other workloads, including claims and program integrity workloads such as redeterminations and medical Continuing Disability Reviews (CDRs).

- Some customers are convinced that Social Security employees are behind the scam calls, and thus view our staff with distrust. This further erodes the confidence the American public has in our agency and the federal government.

- At the teleservice center, customer service representatives are constantly receiving calls that a member of the public received a call from a Social Security employee stating their SSN has been suspended. The number of calls on this issue often increases the wait time for other calls in queue.

From a broad perspective, staff in Social Security field offices and teleservice centers has decreased by 2,530 permanent employees in the last 10 years. Over this same period, Operations employees have been processing more work, with dated technology and complicated policies. With Commissioner Andrew Saul's commitment to improving public service on the front lines, the agency must be as efficient as possible and devote as many front-line resources as necessary to serving the core mission of our agency.

Social Security serves as Maine's largest, most vital component of the social safety net. We are facing unprecedented challenges and this is not the time for the residents of Maine and the rest of the American public to lose faith in the largest, most successful social insurance program in the world. Your constituents expect and deserve our assistance. As the face of the federal government, we have a duty to maintain the public's faith and trust in both the Social Security Administration and federal government. It is challenging for Social Security to keep pace with the fraudsters and provide service to the American public who fall victim to these types of scams. It is more important than ever for the agency and Congress to protect the residents of Maine and take action to eliminate these efforts by fraudsters.

On behalf of the National Council of Social Security Management Associations, thank you for the opportunity to be here today and submit this testimony regarding efforts to protect seniors from impersonation scams. National Council members are not only dedicated Social Security employees, but are also personally committed to the mission of the agency, providing the best service possible to your constituents. We want to ensure that Maine residents and the American public have faith and trust in the Social Security Administration. The public needs reassurance that they will not fall victim to those trying to impersonate Social Security employees.

We respectfully ask that you consider our comments and appreciate any assistance you can provide in ensuring the residents of Maine and the rest of the American public receive the critical and necessary service they deserve from the Social Security Administration without fear of compromising their information.

CITY OF PHILADELPHIA

Office of the Managing Director
BRIAN ABERNATHY
Managing Director

1401 John F. Kennedy Boulevard
Suite 1430
Philadelphia, PA 19102-1683

That's Not the Government Calling:
Protecting Seniors from
the Social Security Impersonation Scam

Testimony before the
Senate Special Committee on Aging
January 29, 2020
9:30 am
Dirksen Senate Office Building
Room 562

Good morning Senators and thank you for inviting me to speak today. As a government official, public interest attorney and nonprofit leader who has advocated for older Americans for more than 30 years, I am pleased to present testimony on the Social Security impersonation scam and some ideas on solutions and best practices for reducing the vulnerability of older Americans.

I am a proud Philadelphian and appreciate Mayor Jim Kenny's leadership in improving economic opportunities and public safety for all Philadelphians. Senator Casey, Senator Collins and this Committee continue to shine a light on the critical needs of older people in our country. We are proud to have Senator Casey represent us in Washington and on this important Committee.

I am currently the Executive Director of the Mayor's Commission on Aging in Philadelphia where almost 294,213 60+ adults live and work.[1] Locally, nationally and globally, people are living longer, and the trend shows no sign of changing. The 'longevity bonus' as some leaders call it, demands a new approach to our way of thinking. Philadelphia's seniors are a diverse and culturally vibrant part of our neighborhoods and many live with family and loved ones in multigenerational settings. However, nearly 1 in four or 24% of older Philadelphians living alone see friends or relatives less than once a week.[2] This can lead to isolation and vulnerability and should be considered when developing interventions to help protect against fraud. Philadelphia is also home to the largest percentage of seniors and poorest overall population among the top ten American cities.[3]

The Social Security Impersonation Scam

In 2018, the Social Security impersonation scam was just making it into the top 10 of scams according to this Committee's exemplary work in responding to and cataloguing scams targeting seniors. By 2019, it had leaped to the top – so that it by far passed the IRS impersonation scam in frequency. It was number one in both Pennsylvania and the nation! The very nature of the Social Security impersonation scam is to trick the victim of this crime into believing that the caller is from the Social Security Agency and is trying to assist or protect the senior from the loss of Social Security benefit. This cynical approach is working, and we must stop the devasting damage that is occurring.

Using robocalls or live callers, fraudsters pretend to be government employees and claim that identity theft has occurred or that there is another problem with one's Social Security number, account, or benefits. They may threaten arrest or other legal action, or may offer to increase benefits, protect assets, or resolve an identity theft. They often demand payment via retail gift card, cash, wire transfer, internet currency such as Bitcoin, or pre-paid debit card.[4]

---

[1] **Source:** US Census 2018 ACS 5-Year Survey (Table S0101)

[2] *Older Adults and Service Utilization in Southeastern Pennsylvania.* Data Findings. Community Health Database, 20 October 2008. Web. 10 October 2012. http://www.chdbdata.org/datafindings-details.asp?id=63.

[3] A report from the PEW Charitable Trusts, November 2017, Philadelphia's Poor: Who they are, where they live, and how that has changed. See https//www.pewtrusts.org/-/media/assets/2017/11/pri_philadelphias-poor/pdf

[4] https://blog.ssa.gov/category/fraud-2/

We know that real SSA will never tell you to wire money, send cash, or put money on a gift card, but in a moment of concern, seniors may believe the scam is legitimate and act to protect their valuable Social Security benefit. The Social Security imposter scam is not just the Committee's top scam of 2019, it is the number one scam reported to the FTC currently. [5] People filed nearly 73,000 reports about Social Security imposters in the first six months of 2019, with reported losses of $17 million.[6]

Addressing the Social Security Impersonation Scam

In partnership with the FTC and SSA, the CFPB has already created a targeted education piece to share with friends and family. This is an important step towards raising awareness of the Social Security impersonation scam among seniors. The language is clear and easy to understand.

> Scams involving your Social Security number and benefits are on the rise!
> Here are the facts:
> Government employees will not threaten to take away benefits or ask for money, gift cards, or personal information to protect your Social Security number or benefits.
> Scammers can fake your caller ID. So, don't be fooled if the call seems to be from the SSA or the SSA Inspector General's Fraud Hotline number.
> If a caller asks for your Social Security number, bank account number, or credit card information, hang up. Report Social Security phone scams to the SSA Inspector General online at oig.ssa.gov. Visit identitytheft.gov/ssa for more tips[7]

Recommendations for the Future

It would be helpful to create a federal advisory council charged with bringing together the key government officials, industry representatives, advocates and consumer representatives to develop model educational materials for retailers, financial institutions and wire transfer companies to use in stopping scams on seniors. One thing we can be sure of, these kinds of scams will continue. The representations may change over time, but the focus on targeting vulnerable older Americans will not.

The Stop Seniors Scams Act, sponsored by Aging Committee Ranking Member Bob Casey (PA) and Commerce Subcommittee on Manufacturing, Trade and Consumer Protection Chairman Jerry Moran (KS), does just that. It further recommends that the advisory council:

- Collect and develop model educational materials for retailers, financial institutions and wire transfer companies to share with their employees;
- Examine ways that these businesses can use their platform to educate the public on scams;
- Provide additional helpful information to retailers, financial institutions and wire transfer companies as they work to prevent fraud affecting older adults; and

---

[5] https://www.consumer.ftc.gov/blog/2019/09/social-security-not-trying-take-your-benefits
[6] Ibid.
[7] https://pueblo.gpo.gov/CFPBPubs/CFPBPubs.php?PubID=13439

- Publicly report information about the newly created model materials as well as recommendations, dissenting views and findings of the Advisory Council.

The Consumer Financial Protection Bureau has created Money Smart for Older Adults (MSOA) in recognition of the reality that older adults have been and continue to be prime targets for fraudsters. MSOA, Version 2.0[8] is also available in Spanish. MSOA, Version 2.0, raises awareness of common frauds and scams and encourages older people to recognize the scams before they lose money to them. The information can be delivered in brief segments over time in settings like senior community centers. It contains an Instructor Guide with a corresponding PowerPoint presentation and allows senior service providers, legal professionals, financial service professionals, and community volunteers to lead the presentation. It could form the basis for the educational materials that the Senior Scams Act references above.

It also would be helpful for the Social Security Agency's OIG to lead a multi-agency task force for dealing with the problem and more aggressively target enforcement actions to root out the perpetrators of this abuse and fraud against Social Security recipients.

Outreach and education like the successful Senior Medicare Patrol (SMP) conducted in every state could be replicated with a focus on Social Security scams. The following brief description of the program follows:

- The SMP program model is one of prevention. SMPs have educated Medicare beneficiaries since 1997 to scrutinize their medical statements. Though beneficiaries have several avenues they can take to report fraud, such as the Office of Inspector General (OIG) hotline or 1-800-Medicare, some beneficiaries choose to report fraud to the SMP. In these cases, SMPs refer the complaint to the appropriate entity.
- The SMP projects receive grants from the Administration for Community Living (ACL) to recruit and train retired professionals and other older adults, often Medicare recipients themselves, to prevent, recognize, and report health care fraud, errors, and abuse. Local non-profits and agencies manage the programs and SMP team members then participate in outreach events to help educate Medicare and Medicaid beneficiaries to do the same.
- The SMP projects reported $15,136 in expected Medicare recoveries and $5,734 in expected Medicaid recoveries. Cost avoidance totaled $602,063, while savings to beneficiaries and others totaled $27,689. Further, additional Medicare expected recoveries totaled $11.9 million.
- The OIG reports that expected recoveries to Medicare and Medicaid attributable to the projects from 1997 through 2018 were $119.7 million. Total savings to beneficiaries and others were approximately $7.1 million. Total cost avoidance on behalf of Medicare, Medicaid, beneficiaries, and others was $10 million.[9]

[8] https://www.consumerfinance.gov/practitioner-resources/resources-for-older-adults/protecting-against-fraud/
[9] https://www.smpresource.org/Content/What-SMPs-Do/SMP-Results.aspx

The Department of Justice, Fraud Division, should conduct a training for lawyers representing victims of the Social Security impersonation scam to insure their identity is secured and that they are less vulnerable to scams in the future.

Respectfully submitted,

NORA DOWD EISENHOWER
Executive Director
Mayor's Commission on Aging

Questions for the Record

U.S. Senate Special Committee on Aging
"That's Not the Government Calling: Protecting Seniors From the Social Security Impersonation Scam"
January 29, 2020

Questions for the Record
Hon. Andrew Saul

Senator Robert P. Casey, Jr., Ranking Member

Question:

SSA is responsible for several key Medicare functions, including providing basic education about when and how to sign up for Medicare and processing Medicare enrollment. Increasingly, people new to Medicare are delaying retirement beyond age 65. Without adequate, advance notification, these individuals often lack sufficient information on when and how to sign up for Medicare. The consequences of enrollment missteps, particularly in Medicare Part B, can be significant and may include lifetime late enrollment penalties as well as lengthy gaps in coverage. In my October 2018 Questions for the Record, I asked you to commit to a series of actions to improve the Medicare enrollment process. Please provide an update on the actions you have taken since assuming office to:

a. Evaluate SSA's processes and procedures for educating individuals approaching Medicare eligibility about basic Medicare enrollment rules, including how Medicare benefits coordinate with other forms of insurance, Part B enrollment periods and coverage start dates and eligibility for and enrollment in Medicare low-income support programs;
b. Strengthen notification and resources for individuals nearing Medicare eligibility; and
c. Ensure that SSA appropriately balances online educational initiatives pertaining to Medicare enrollment with both paper mailings and in-person assistance.

Created through federal law, equitable relief is an administrative process that allows people with Medicare to request relief from SSA in the form of immediate or retroactive enrollment into Medicare Part B and/or the elimination of a Medicare Part B Late Enrollment Penalty (LEP). It is my understanding that SSA does not currently collect or retain information on equitable relief cases, including the number of cases processed, the outcomes of these requests or information on the basis for these requests. In my October 2018 Questions for the Record, I asked you to commit to collecting and disseminating information regarding Medicare equitable relief, you responded that once confirmed you would review data SSA collects and maintains to determine whether it addresses my questions. In your role as Commissioner, please answer the following questions:

d. Will you commit to collecting basic, state-by-state data on equitable relief cases (including the number requested, the outcome of the requests, and the basis for requests) and ensure that data is made available to my office?
e. Will you ensure this data collection process includes information on current and former Marketplace enrollees who seek time-limited equitable relief?
f. Will you provide my office with information on how SSA manages, processes and decides equitable relief requests?
g. Will you provide information to my office on the extent to which SSA trains field office staff regarding cases of equitable relief and special enrollment periods?

During the hearing, you mentioned mailers and noted that the Social Security Administration is adding a scam message to certain mailers to alert individuals to the threat of Social Security imposter scams. Please provide information on the specific Social Security mailers that will have new content, the newly added content as well as an estimate of the funds SSA expended to develop and supply this content. Where possible, please provide a copy of the exact content added.

In your confirmation hearing and in your responses to Questions for the Record from October 2018, you stated that reducing wait times for Social Security Disability Insurance (SSDI) application decisions and hearings were among your top priorities. While wait times and backlogs have fallen relative to their recent peak, wait times remain unacceptably long in many areas of the country and my home state of Pennsylvania.

h. Since your confirmation, what specific steps have you taken to reduce wait times for decisions and hearings for SSDI applicants?
i. What additional steps do you intend to take to further reduce these wait times?
j. What are SSA's current targets for wait times and by when does the agency believe it will achieve them?
k. Why is SSA proposing through the Rules Regarding the Frequency and Notice of Continuing Disability Reviews (RIN 0960-AI27) to spend valuable administrative resources on conducting 2.6 million more continuing disability reviews over the next ten years when agency resources are needed to address unacceptable wait times?

In the FY 2020 appropriations package, Congress urged SSA to develop a telework plan for operations employees as quickly as practicable. This came after SSA ended a previous telework program for employees in SSA's operations components in November, 2019, despite 44 Senators and workers' representatives asking the agency to reconsider.

l. What progress have you made in developing a new telework plan for operations employees and what is the timeline for its introduction?
m. Are you consulting with the unions representing SSA operations employees in the development of this telework plan?

You recently announced the hiring of 1,100 front line employees to provide service on SSA's National 800 Number and in processing centers. All measures that will help to restore essential SSA services and reduce wait time are needed, including ensuring that SSA is adequately staffed. To better understand how these hires may assist in improving customer service, can you please answer the following questions:

n. What were the total staffing levels of field offices, processing centers and teleservice centers in each of the past 10 fiscal years? How many hires were made in each fiscal year and how many workers were lost to retirement or other forms of attrition in each fiscal year?
o. How many workers does SSA anticipate losing to attrition in FY 2020 in field offices, processing centers and teleservice centers?
p. Does SSA intend to hire any additional field office staff?

The Wall Street Journal published an article on January 10, 2020, detailing an unreleased SSA proposed rule that would revise how the agency considers individuals' age, education and work experience when

evaluating whether they are eligible for disability benefits. The changes described in the article could be extremely harmful to hundreds of thousands of Americans who are no longer able to work due to a disability and are seeking to claim disability benefits, they have earned. Given the importance of this potential rulemaking to Americans with disabilities, can you please answer the following questions:

q. When did the collection of information and drafting of this proposed rule begin and what level of funds and man hours has SSA expended on the development of this rule thus far?
r. What sources of information and data is SSA drawing upon in the development of this proposed rule? What, if any, organizations or individuals outside of the agency has SSA consulted with concerning this proposed rule?
s. The Wall Street Journal article states that SSA officials have met frequently with White House and OMB officials to discuss the development of this rule. What White House, OMB and SSA officials have taken part in these meetings and how frequently have these meetings occurred?
t. Is SSA consulting with stakeholder and advocacy organizations, such as those that represent individuals with disabilities in the disability adjudication process, to inform the agency's decision-making process?

Senator Tim Scott

Question:

Commissioner Saul, thank you for your testimony. We should all work tirelessly to protect vulnerable populations from fraud, and I appreciate your agency's work in addressing the issue of phone scams targeted at seniors. I believe SSA has an important role to play it helping to mitigate other forms of fraud as well. As you know, I authored the Protecting Children from Identity Theft law, which passed as part of S. 2155, our landmark regulatory relief and consumer protection legislation from last Congress. As your agency continues to engage with me and the law's other bipartisan champions, along with key stakeholders, on implementation, I want to thank you for your progress, but also to highlight areas where questions and concerns remain, particularly with regards to electronic consent and issues of legal authorities. While I am confident that we can work proactively and collaboratively to ensure effective implementation that will meaningfully combat synthetic identity theft, I would direct your agency to the following areas as you continue to strive to align execution with legislative intent.

- Providing for consumer consent to be received electronically, in accordance with the Electronic Signatures in Global and National Commerce Act (E-SIGN), in order for a financial institution to access the Electronic Consent Based SSN Verification System (eCBSV) is at the heart of the Protecting Children from Identity Theft law (referred to by SSA as the "Banking Bill"). That said, aspects of the draft user agreement and additional electronic consent requirements document SSA recently presented appear to reinterpret the intent of the Banking Bill, as well as the E-SIGN Act.

  As I noted during Senate consideration of the Banking Bill, nothing in this law regarding consumer consent should add friction to the consumer experience when applying for a financial product or service, with the goal to be to inform consumers of the possible inquiry to the eCBSV system and allow them to provide consent in a way consistent with established – and regulated – practices throughout the industry. SSA's proposed approach to consent runs the risk of imposing significant operational burdens onto end users. Will you commit to working with my staff, the offices of my bipartisan cosponsors from the bill, and the future

users of the eCBSV to ensure the final consent requirements adhere to the law and our legislative intent?

- In an effort to deter fraud and abuse, I outlined specific audit authorities granted to SSA through our legislation in the Banking Bill, which include, a) ensuring that consent is being captured and retained correctly, b) ensuring that companies are integrated properly within your system, and c) ensuring that no one is defrauding the system. The legislation did not authorize SSA to assume any functions beyond those specifically and narrowly connected with eCBSV, consumer consent forms, and the responses given by SSA back to financial institutions.

However, your agency's draft user agreement would grant SSA a number of the regulatory and examination authorities over bank data and privacy practices that are the jurisdiction of federal banking regulators, exceeding what Congress articulated in the Banking Bill. Will you commit to working to narrow the scope of your draft user agreement to only the specific authorities outlined in the Banking Bill?

Senator Doug Jones

Question:

We've discussed in previous hearings how fraudsters often use robocalls and scams to not only solicit money, but also to get victims' personal information. This information is then used to steal from individuals, their families, and even the federal government. For example, tens of thousands of Americans fall victim each year to tax refund fraud. Chairman Collins and I worked together to pass our *Taxpayer Identity Protection Act* this summer, which will create an extra layer of protection for Americans by expanding IRS's Identity Protection PIN program. Is there something analogous to the IP PIN program that SSA could use to protect customers and restore trust?

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

U.S. Senate Special Committee on Aging
"That's Not the Government Calling: Protecting Seniors From The Social Security Impersonation Scam"
January 29, 2020

Questions for the Record
Hon. Gail S. Ennis

Senator Doug Jones

Question:

We've discussed in previous hearings how fraudsters often use robocalls and scams to not only solicit money, but also to get victims' personal information. This information is then used to steal from individuals, their families, and even the federal government. For example, tens of thousands of Americans fall victim each year to tax refund fraud. Chairman Collins and I worked together to pass our *Taxpayer Identity Protection Act* this summer, which will create an extra layer of protection for Americans by expanding IRS's Identity Protection PIN program. Is there something analogous to the IP PIN program that SSA could use to protect customers and restore trust?

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

U.S. Senate Special Committee on Aging
"That's Not the Government Calling: Protecting Seniors From The Social Security Impersonation Scam"
January 29, 2020

Questions for the Record
Ms. Nora Dowd Eisenhower

Senator Doug Jones

Question:

Your testimony highlighted the success of peer-to-peer programs like the Senior Medicare Patrol. In previous hearings, we have also discussed the importance of engaging younger generations in prevention efforts. Have you considered leveraging multigenerational programs to address and raise awareness about such issues? What information should younger generations know about scams so that they can help to "break the spell"?

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

○