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.

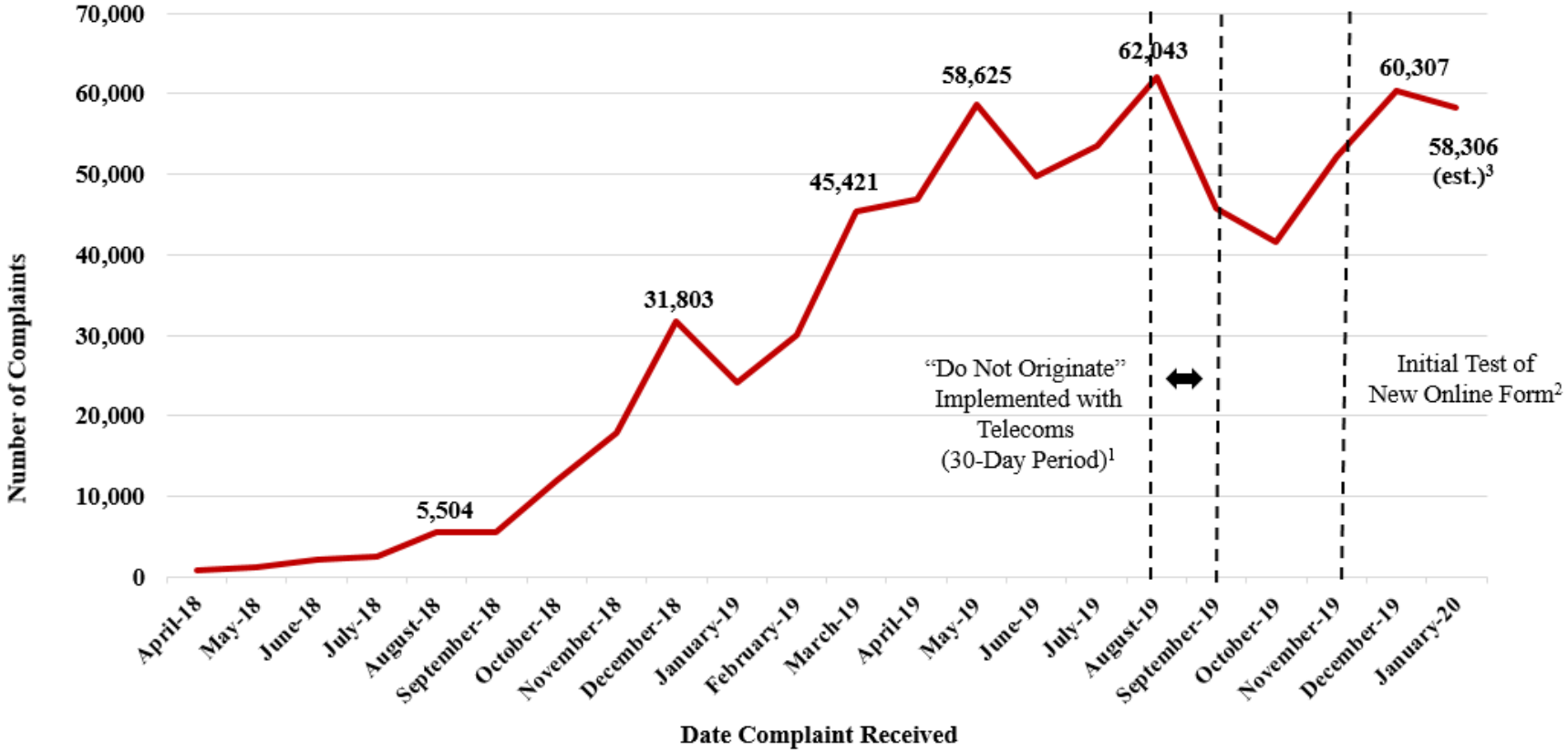
Conclusion

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.

Date Prepared: January 24, 2020