

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. 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. 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.

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 <u>number one scam reported</u> 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 tips⁷

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 2.0⁸ 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.

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