**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.