Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

United States Senate
Special Committee on Aging

Statement for the Record

Made in China, Paid by Seniors: Stopping the Surge of International Scams

Michelle L. Anderson
Assistant Inspector General for Audit
as First Assistant

Social Security Administration
Office of the Inspector General

January 14, 2026

Chairman Scott, Ranking Member Gillibrand, and members of the Committee. I want to thank the Special Committee on Aging for holding today's hearing entitled "Made in China, Paid by Seniors: Stopping the Surge of International Scams."

The Social Security Administration (SSA) Office of the Inspector General (OIG) is a key federal player in the fight against government imposter scams. Many of these scams originate from overseas and reach our American shores, stealing significant amounts of money from Americans.

In 2024, according to the Federal Trade Commission (FTC) consumers reported losing $12.5 billion to scams, including government imposter scams. FTC estimates that, when adjusted for underreporting, Americans may have actually lost a staggering $158 billion to scammers.

Scams are known to be linked to transnational criminal organizations. National security and economic stability are at serious risk. International scammers are viciously attacking Americans, and we are all vulnerable.

Hard-earned money from the American public leaves the United States and is being utilized to fuel their criminal enterprises, which according to reports from the FTC and the Federal Bureau of Investigations (FBI), may often involve organized crimes such as drug and human trafficking. Moreover, scammers will also draw Americans into their crimes to facilitate the transfer and movement of stolen funds.

Hearings, such as one today, provide an important reminder to every American to be vigilant and to protect their money and personal information from scammers. Individual awareness and skepticism when contacted by telephone, text, email, social media, and even U.S. mail ploys, is the first line of defense in identifying and preventing a scam.

Scammers exploit human emotion; fear, intimidation, trust, urgency, loneliness, sympathy, and even hope can be used to manipulate people into complying with demands. These criminals are relentless in their efforts to gain access to Americans' money or personal information. Even when scammers fail to obtain direct payment from their victims, they use Americans' identities and monetize them for criminal activity.

Social Security scams are widespread across the country and reach people of all ages. However, seniors are disproportionally affected. As noted in SSA OIG's most recent *Scam Update to Congress*, individuals of all ages report scams, but individuals aged 70 and over report significantly higher financial losses to scams.

The goal is to prevent Americans' personal information and hard-earned money from leaving the United States, because retrieving this information or lost financial assets from malign actors outside the United States is nearly impossible.

The scams can be complex: a scammer contacts an American and tells them they must pay a fine or provide information to avoid arrest or other legal action, resolve a Social Security number problem, or increase a benefit. They demand money using difficult to trace forms of payment, such as cash, retail gift cards, pre-paid debit cards, gold bars, or cryptocurrency. Scammers often apply immense pressure and quickly escalate threats to frighten victims into complying. Scammers have emailed fake letters that appear to come from Social Security, utilizing official looking letterhead or the publicly available names of actual SSA and SSA OIG employees, to convince potential victims of their legitimacy.

While SSA OIG has seen a precipitous decline in reports of SSA-related imposter scams from 2020 to the present, SSA-related scams remain a top-reported government imposter scam. In fact, according to FTC data, SSA remains the top federal agency used in schemes by criminals to defraud Americans.

SSA OIG has taken a multi-disciplinary approach to combatting SSA-related government imposter scams. For five years, SSA OIG has investigated emerging major fraud schemes against SSA programs and operations, including government imposter scams. Investigating large-scale organized fraud often requires a multi-disciplinary effort with enhanced legal and analytical capabilities, and coordination with multiple law enforcement agencies around the country. OIG works zealously to develop leads, disrupt the scams, and provide evidence for criminal prosecutors. For example, our work with federal and state partners has led to the prosecution and sentencing of multiple individuals involved in telephone imposter scams originating from overseas call centers.

SSA OIG agents and attorneys also notify domestic gateway telecommunications providers (who serve as intermediaries between foreign providers and downstream American telecom carriers and pass-through millions of calls daily) of their potential civil liability under a consumer protection law within the *Social Security Act*.[1] In doing so, SSA OIG attorneys educate these domestic gateway providers on the applicability of this statutory provision, encourages proactive techniques to identify and block transmission of scam calls both domestically and internationally, and, where appropriate impose fines.

Artificial Intelligence (AI) is rapidly becoming a primary driver of emerging technologies and is impacting society in ways the public and private sectors are just beginning to understand. China and other nations are in a race with the United States to develop and implement AI. While criminals have used AI to increase the volume and speed of their criminal activities, AI has also become an important technology in fraud detection. It is possible to thwart fraud attempts by using large data sets to continuously train fraud detection algorithms to predict and recognize anomalous patterns indicative of fraud in the private and public sectors.

AI will continue to be a powerful tool to support the Federal Government's ability to detect and prevent the fraudulent disbursement of taxpayers' dollars. AI is also a formidable tool for international criminals to engage in widespread and repeated scams at a low cost. Criminals use AI to make scams easier and faster to execute, the deceptions more credible and realistic, and ultimately, the scam more profitable.

SSA OIG is concerned about how scammers will continue to utilize AI to increase the frequency and sophistication of scams against Americans. SSA OIG's goal is to be at the forefront by leveraging AI to detect fraud, improve decision making, and learn rapidly how AI can be used in new and emerging ways to commit malicious behavior.

[1] Section 1140 of the *Social Security Act* (42 U.S.C. § 1320b-10), as amended, protects the public from advertisements, solicitations, and other communications (including websites and scam telephone calls) that may convey the false impression SSA approved, endorsed, or authorized the communication. It also prohibits the reproduction and sale of SSA publications and forms without authorization and places restrictions on charging for services SSA provides to the public for free.

SSA OIG established a Task Force to study AI and related technology. From this effort, SSA OIG is working to determine the tools, processes, and staffing needed to detect, investigate, and deter AI-related fraud and to leverage AI in fighting fraud. SSA OIG will continue to work with longtime federal law enforcement partners to stay current in the detection, investigation, and deterrence of AI-related fraud. The goal of the SSA OIG AI Task Force, through collaboration with the agency, is to also work to ensure SSA unwraps the potential transformational impact of AI to benefit the American public in a way that balances enhanced customer service and limits the risk of fraud.

SSA OIG also collaborates with SSA through the National Anti-Fraud Committee (NAFC), a partnership of senior leaders dedicated to combating fraud, waste, and abuse in SSA programs. Meeting quarterly to share information and develop actionable strategies, the NAFC also hosts an annual multi-day summit for SSA and SSA OIG subject matter experts, fostering collaboration, addressing challenges, and identifying vulnerabilities.

NAFC has been the breeding ground of ideas for the need to use AI to fight fraud, waste, and abuse and the need to fight AI-related fraud. Following each summit, SSA OIG and SSA mutually agree upon action items to enhance the efficiency and effectiveness of agency operations. The NAFC summits have been critical in leading to significant improvement in fighting fraud waste, and abuse and promoting the efficiency and effectiveness of SSA's programs and operations.

In fact, following the Fiscal Year 2023 NAFC summit, SSA and SSA OIG agreed to establish the NAFC AI Subcommittee, which consists of the SSA OIG AI Task Force members and SSA's AI Core Team, including its Chief AI Officer. The NAFC AI Subcommittee meets quarterly and discusses SSA's compliance with M-25-21, its AI Strategy and Compliance Plain, its current inventory of AI-use cases, and AI-use cases in development. It also explores risk assessments and identifies vulnerabilities in SSA's AI-use cases, contributing to enhanced oversight through improved fraud detection and mitigation strategies. Additionally, the Task Force has assisted SSA in spotlighting and addressing AI threats, mostly identified through NAFC-related activities.

Mr. Chairman, scams against Americans erode the public's trust in SSA, and in the Federal Government overall. SSA OIG will continue to engage with agencies like the FTC and Federal Communications Commission (FCC), who have proven capable partners in our fight against government imposter fraud. SSA OIG meets regularly and collaborates with SSA to understand how the agency plans to use AI in its operations, and will review any applicable risk assessments, vulnerabilities, and/or efficiencies gained utilizing AI in SSA programs. Additionally, with our oversight tools, we plan to assist SSA to address AI threats to the agency and to Social Security numberholders.

SSA OIG is committed to educating the public about scams by individuals pretending to be from SSA or SSA OIG to empower the public to identify and prevent the scams themselves. SSA OIG educates the public through a multidisciplinary public awareness campaign. Along with public and private partners, the media, the United States Congress, and agencies across the Federal Government, SSA OIG works tirelessly to try to reach every American to reduce the number of people who lose money and personal information to these pervasive and insidious scams.

I, especially, want to take a moment to recognize Chairman Scott and Ranking Member Gillibrand and members of the Committee who have supported SSA OIG's annual National Slam the Scam Day. In 2025, Chairman Scott and Senator Kelly took the lead to introduce and

pass by unanimous consent the bipartisan resolution S.J. Res 118 during National Consumer Protection Week.

National Slam that Scam Day is the centerpiece of SSA OIG's year-round public-awareness campaign. National Slam the Scam Day, as this hearing is doing today, educates the public about the tactics scammers use and encourages the public to "slam" scammers. Providing awareness and tips for spotting scams is a major thrust of the National Slam the Scam Day public awareness campaign.

Education and outreach continue to be a powerful tool, empowering consumers to protect themselves and their communities from scams. SSA OIG will continue to urge Americans to disconnect from interactions with scammers, whether on the telephone, via text, social media, or email. It is our goal to keep Americans well informed of the tactics scammers use, new and emerging scam trends, and available resources.

SSA and SSA OIG's joint website www.ssa.gov/scam shares resources, tips, and alerts and allows individuals to report Social Security-related scams. Americans can help SSA OIG by continuing to report scams, providing valuable data for investigative leads and targeted outreach. SSA OIG will continue to urge each American to be cautious of any contact supposedly from a government agency telling you about a problem you do not recognize.

Real government officials will NEVER:

- Threaten arrest or legal action against you unless you immediately send money;
- Promise to increase your benefits or resolve a problem if you pay a fee or move your money into a protected account;
- Require payment with gift cards, prepaid debit cards, wire transfer, Internet currency, gold bars, or by mailing cash; or
- Try to gain your trust by providing fake "documentation," false "evidence," or the name of a real government official.

Unfortunately, the scams and the scammers continue to evolve, and we at SSA OIG always expect they will soon move on to new tactics and techniques. Further, we are constantly monitoring what transnational criminal organizations are doing to infiltrate and commit scams against Americans.

These scammers have robbed too many individuals of their hard-earned savings, and the Federal Government must continue to leverage resources across agencies and use innovative approaches to stop the scams and protect Americans. At some point soon, most Americans will have experienced, or know someone who has experienced, losing money or personal information to a scam.

Thank you for holding this hearing today to discuss ways to protect Americans from these scams. Raising public awareness, without question, is one of the most effective ways to combat scams. By educating all Americans, we can help them identify, prevent, and report scams. Thank you again for the opportunity to submit the statement for the record.