



# QUARTERLY SCAM UPDATE

Issue 17

**OFFICE OF THE INSPECTOR GENERAL  
SOCIAL SECURITY ADMINISTRATION**

April 1, 2025 – June 30, 2025

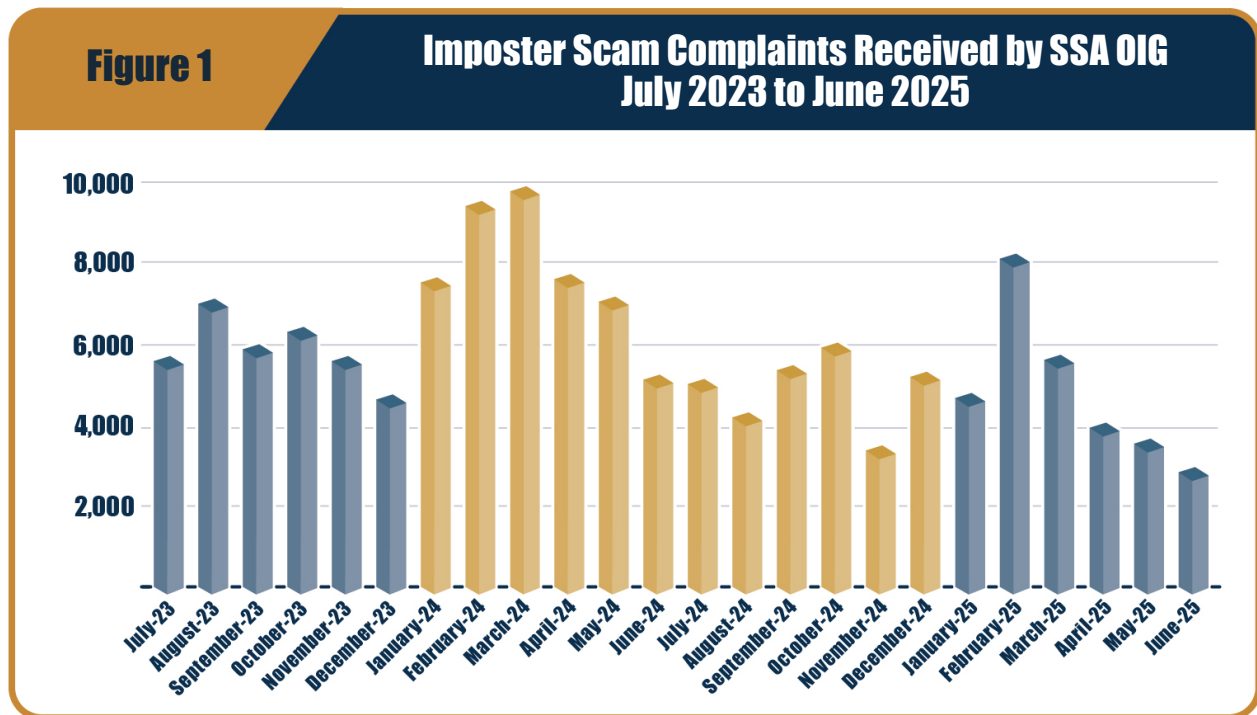
## **Social Security-Related Scams**

The Social Security Administration (SSA) and SSA Office of the Inspector General (OIG) continue to receive reports of scammers impersonating government employees or alleging a Social Security-related problem to steal money or personal information from victims.

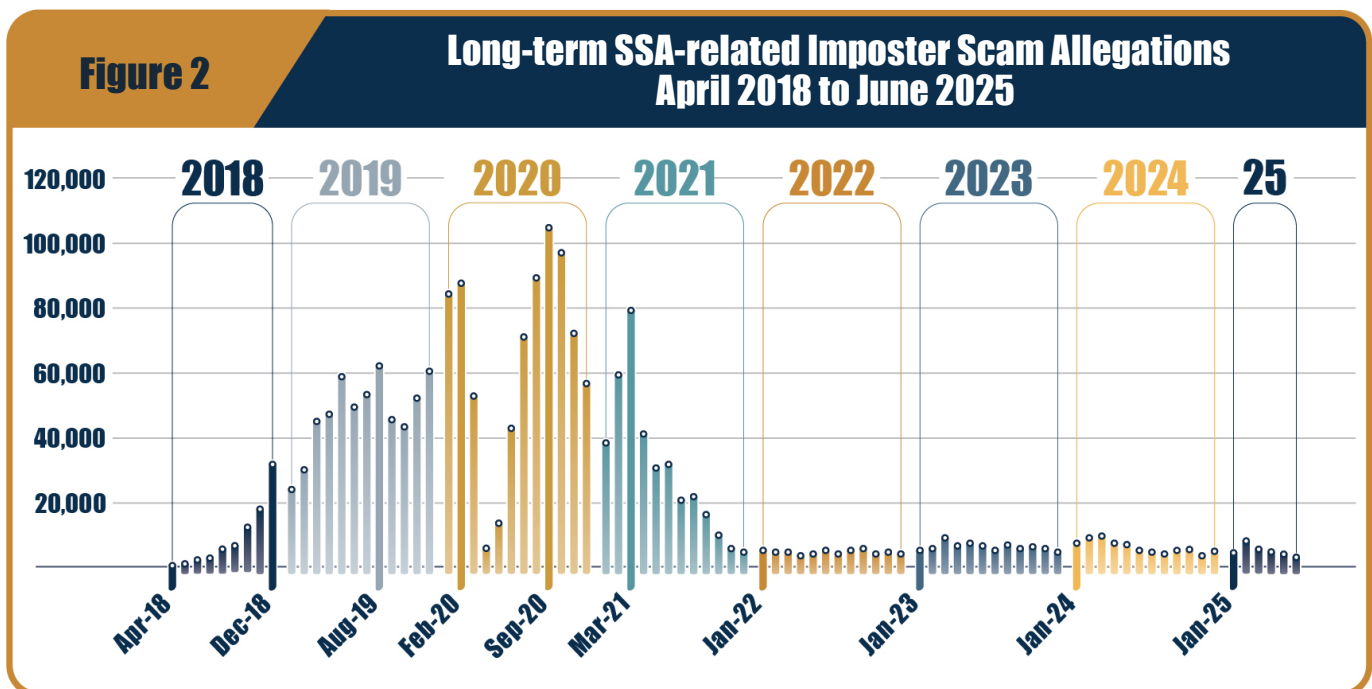
Since October 2019, SSA OIG has shared information on its efforts to combat Social Security-related scams with the U.S. House of Representatives Committee on Ways and Means, Subcommittee on Social Security; U.S. Senate Committee on Finance; and U.S. Senate Special Committee on Aging. SSA OIG began publicly releasing the Quarterly Scam Update in the third quarter of Fiscal Year (FY) 2021 to provide information about these scams and its efforts to combat them.

This report shares information about Social Security-related imposter scam allegation trends in the third quarter (Q3) of FY 2025 (April 1 through June 30, 2025). Examples of SSA and SSA OIG's recent efforts to disrupt and raise awareness of scams are also included.





While scam complaints have fluctuated over the last two years (see Figure 1 above), scams reported to SSA OIG have decreased significantly since 2021 (see Figure 2 below). This aligns with data reported by the Federal Trade Commission (FTC), which shows imposter scam complaints across the government have declined since 2021. However, FTC data also shows a significant increase in government-wide scam reports again in FY 2025. The FTC continues to identify Social Security-related scams as a top reported government imposter scam type.<sup>1</sup> Therefore, while the long-term decline is promising, SSA OIG and SSA remain vigilant in fighting these scams.









1. This information is based on data [reported to the FTC](#) as of August 12, 2025.

SSA OIG receives the majority of Social Security-related scam allegations from its dedicated online scam reporting form and its hotline. While the form states it is for those who “believe [they] have been a victim of a Social Security Administration Scam,” the form also allows individuals to report whether the scam involved the impersonation of officials from federal, state, or local government agencies other than SSA.

**Figure 3**

## Q2 and Q3 FY 2025 Complaint Trends – Percentage of Total Imposter Allegations from the Scam Reporting Form

Complaint Characteristics		Q2 1/1/25–3/31/25	Q3 4/1/25–6/30/25
	The imposter mentioned a problem with your Social Security number	17.4%	19.0%
	The imposter mentioned a problem with your Social Security benefits	18.0%	19.1%
	The imposter used documents or images (such as a federal logo) when communicating with you	23.3%	29.2%
	The scam involved the impersonation of officials from federal, state, or local government agencies other than the Social Security Administration	36.1%	30.9%
	The imposter mentioned a coronavirus or COVID-19 related issue, or referred to a coronavirus or COVID-19 stimulus check, stimulus payment, or economic impact payment	3.7%	1.7%
	None of the Above	49.4%	40.1%

Note: The percentages were calculated based on the total number of allegations each quarter. The percentages do not add to 100 percent because individual allegations may include more than one complaint characteristic.

In Q2 FY 2025, more individuals 50 years of age or older reported financial losses than those under 50 years of age. Figure 4 (below) shows that in Q3 FY 2025, this trend changed. In Q3 FY 2025, 329 individuals under 50 years of age reported losses, compared with 184 individuals 50 years of age and older.

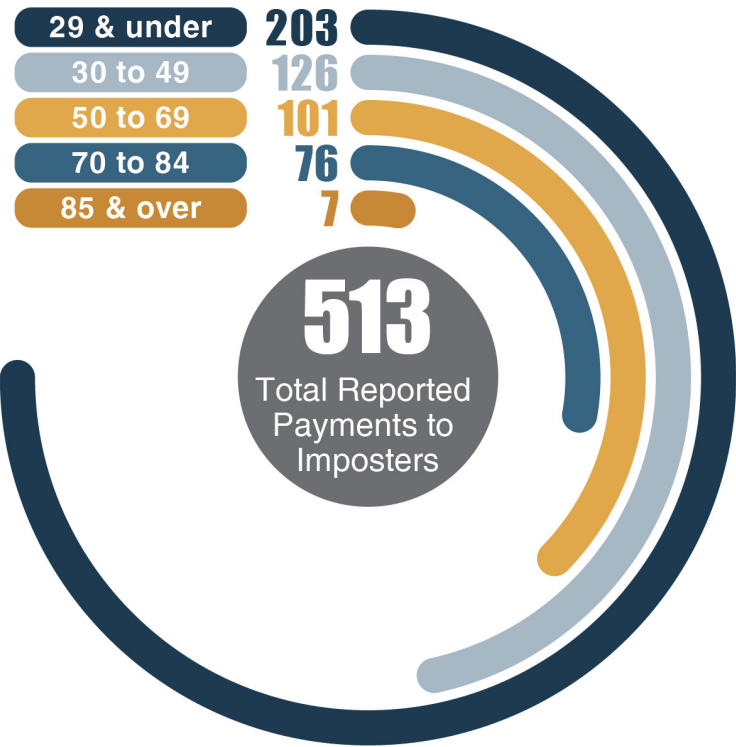


Figure 4  
**Number of Reported Payments to Imposters, by Reported Age**  
4/1/2025 – 6/30/2025

In Q2 FY 2025, individuals 70 years of age and over reported higher average losses than those under 70 years of age. Figure 5 (below) shows that in Q3 FY 2025, this trend continued.

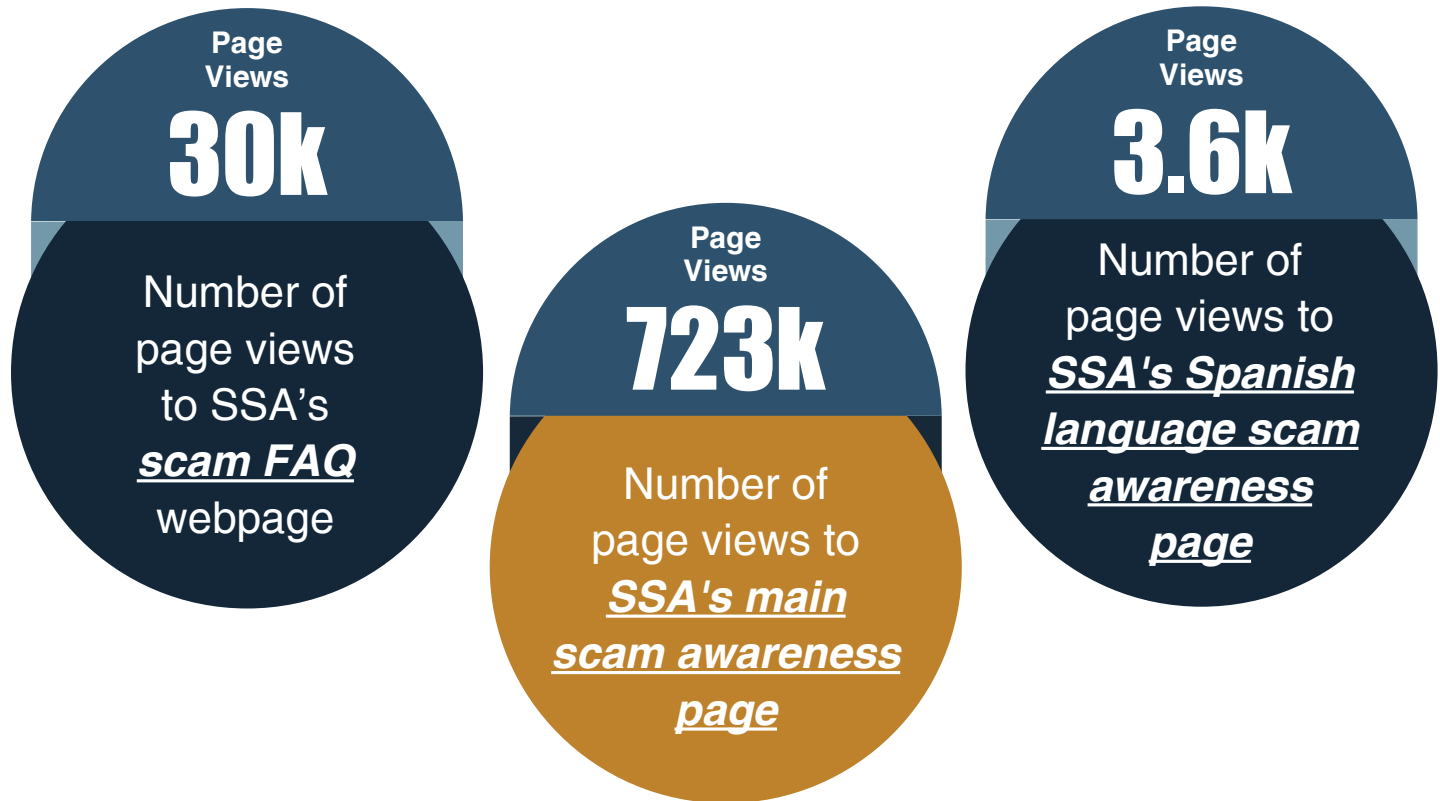


Figure 5  
**Average Dollar Value Reported Payments to Imposters, by Reported Age**  
4/1/2025 – 6/30/2025



## Q3 FY 2025 Website Page Views and Social Media Impressions

Since the launch of the redesigned SSA and SSA OIG joint scam page on May 19, 2022, there have been **8.1 million page views**. Website page views, clicks, and social media impressions for Q3 FY 2025 are shown below.



SSA's October 2021 *Scam Awareness Public Service Announcement video* (left) generated 1.2 million impressions in Q3 FY 2025.

SSA's November 2023 *video* (right), *How to Spot a Scam*, garnered 2,172 views in Q3 FY 2025.

The *Spanish language version of the video*, *Cómo detectar una estafa*, had 1,228 views during Q3 FY 2025.





## Q3 FY 2025 Additional Internal and External Education Efforts

SSA and SSA OIG engaged in additional outreach and education efforts with members of the public, governmental and non-governmental organizations, and SSA employees to raise awareness of scams targeting U.S. residents. Some examples of these efforts during Q3 FY 2025 included the activities below.



In April 2025, SSA published a broadcast for front line employees to alert them of a scam involving criminal impersonation of SSA OIG agents and other federal law enforcement officials and to provide related anti-scam reminders.

In May and June 2025, two entities that charge fees for SSA-related services voluntarily complied with SSA OIG's request to provide notice more prominently on their websites and marketing materials that SSA provides similar services for free.



In June 2025, SSA OIG reached settlement agreements with:

- o a Social Security disability representation organization that SSA OIG asserted utilized misleading marketing practices.
- o a Pennsylvania resident whom SSA OIG asserted engaged in an electronic media campaign with a fictitious persona leading the public, press, and municipalities into believing that unapproved information and guidance was issued, approved, endorsed, and/or authorized by SSA.
- o a Missouri resident whom SSA OIG asserted sold digital renderings of Social Security number cards through an online marketplace.

Throughout June 2025, SSA displayed scam alert slides (right) on monitors in its field offices about scammers pretending to be hiring personnel or recruiters offering fake remote jobs for SSA.

### SCAM ALERT!



Scammers are pretending to be hiring personnel or recruiters offering fake remote jobs for SSA.

They will try to trick you into sharing personal information such as your Social Security number or bank account under the promise of a "new job" working for SSA.

Be aware of unsolicited job offers through calls, email, text, or social media messages.

**Don't be fooled! Visit [ssa.gov/scam](https://ssa.gov/scam) to learn more.**



On June 20, 2025, InvestigateTV released [an interview](#) with Mary Miller, Senior Advisor for SSA OIG on Social Security-related scams. The interview was distributed to television stations serving 113 markets across the country with a total national audience of nearly 1.4 million viewers.

SSA OIG also provided information for a June 20, 2025, WXYZ Detroit news story, [Why a federal agency is issuing a fresh warning on remote job offer scams](#), which highlighted SSA OIG's June 3, 2025, [scam alert](#) on remote job scams.



During Q3 FY 2025, SSA OIG issued two Scam Alerts. First, on April 1, 2025, SSA OIG issued **Beware of Scam Emails Asking to Download Statements** to warn the public to be aware of emails that appear to be from SSA and include a link to download their Social Security statement. This email is an attempt to lure individuals to fraudulent sites that are not associated with SSA. The first image (right) closely resembles a legitimate Gov Delivery email, making it particularly deceptive.

This is NOT an official SSA notice, nor is it from an official government email address. It does NOT have “.gov” as part of the sender’s address. Government agencies end with “.gov” as part of their official email address. The email states that the individual’s Social Security statement is available for download. These emails are not from SSA and will compromise personal data and likely damage computer systems once access is allowed.

SSA OIG advised the public to always be cautious of responding to or clicking links in unsolicited emails that appear to be from an official government entity, such as SSA, or another federal agency.



Next, on June 3, 2025, SSA OIG issued **Watch Out for Remote Job Scams Claiming to be from SSA** cautioning the public about a growing scam involving fraudulent remote job offers falsely claiming to be associated with SSA or other government agencies. Scammers are posing as hiring personnel or recruiters and offering fictitious remote positions — such as “administrative assistant,” “claims processor,” or “virtual benefits coordinator.” These scammers may use fake SSA email addresses, official-looking documents, or spoofed phone numbers. Scammers may ask for personal

information such as Social Security numbers, banking details, or copies of government-issued IDs. Victims may be told to pay for training materials or computer equipment as a condition of employment. “These criminals are exploiting the desire for remote work by impersonating a trusted government agency,” said Michelle L. Anderson, Assistant Inspector General for Audit, performing the duties of the Inspector General. “We urge everyone to exercise caution, verify job offers, and report suspected scams immediately.”

Read all SSA OIG Scam Alerts [here](#).

Section 1140 of the *Social Security Act*, 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.

The focus of SSA OIG's Section 1140 consumer protection program is prevention and early intervention to minimize harm to the public and SSA's reputation, while also allowing violating individuals and entities the opportunity to bring their operations into compliance with Section 1140. During Q3 FY 2025, SSA OIG's efforts included:



Meeting with an online retailer to proactively prevent third-party sellers from listing unauthorized SSA-emblemmed merchandise on its platform.

Meeting with an entity whose data systems were fraudulently accessed to disseminate SSA-related imposter emails. Upon any such future occurrences, the entity will notify SSA OIG immediately to enable SSA OIG and SSA to alert the public through its communications networks.



Educating an online retailer which subsequently removed unauthorized third-party SSA-emblemmed merchandise from its platform.

Initiating four social media takedown requests for SSA-related imposter accounts.



SSA OIG continued its vigilance in monitoring and responding to SSA-related imposter social media accounts because of the public's vulnerability for harm from social media scams. These imposter accounts can also negatively impact SSA's reputation and ability to effectively communicate via its robust social media program. During Q3 FY 2025, in addition to the four takedown requests, SSA OIG opened numerous inquiries regarding SSA-related imposter social media accounts and other communications.





# OIG.SSA.GOV

---

**Office of the Inspector General**

Quarterly Scam Update | Issue 17 | April 1, 2025 – June 30, 2025

Produced and published at U.S. taxpayer expense