



QUARTERLY SCAM UPDATE

Issue 16

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

January 1, 2025 – March 31, 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.

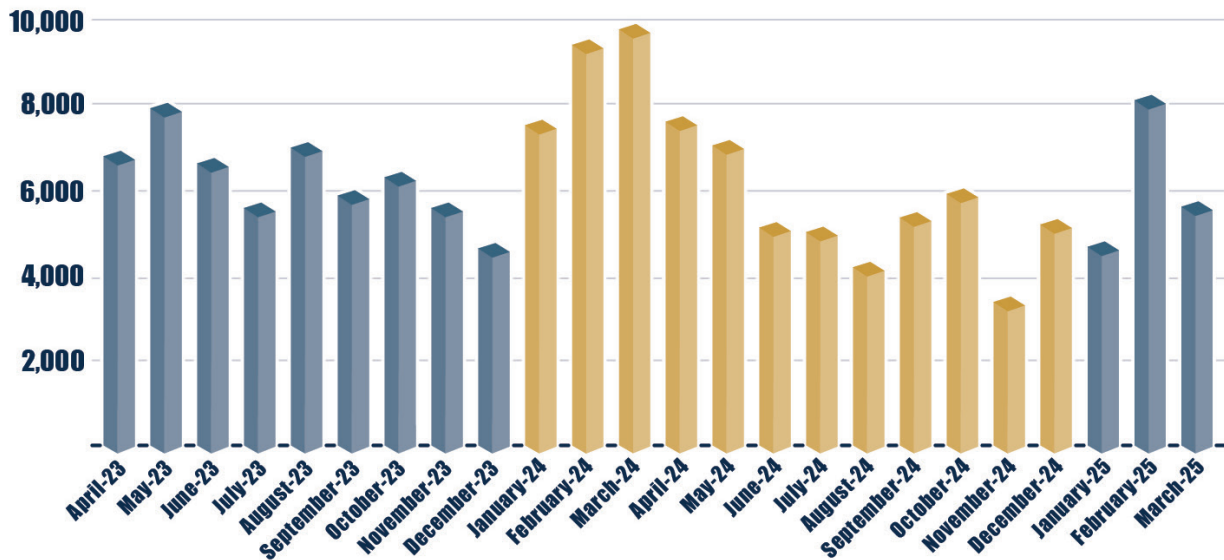
Since October 2019, SSA OIG has shared information on its efforts to combat Social Security-related scams with the U.S. House of Representatives Committee on Ways and Means, Subcommittee on Social Security; U.S. Senate Committee on Finance; and U.S. Senate Special Committee on Aging. SSA OIG began publicly 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 second quarter (Q2) of FY 2025 (January 1 through March 31, 2025). Examples of SSA and SSA OIG's recent efforts to disrupt and raise awareness of scams are also included.



Figure 1

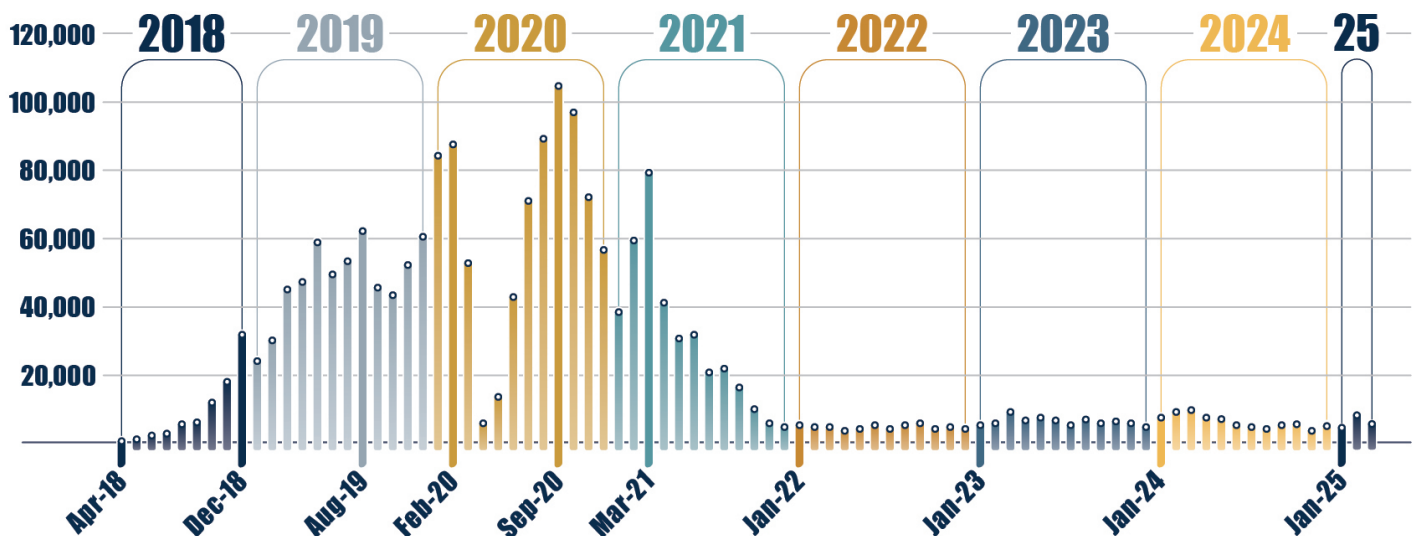
Imposter Scam Complaints Received by SSA OIG April 2023 to March 2025



While imposter scam complaints have fluctuated over the last two years (see Figure 1 above), scams reported to SSA OIG are still down significantly from the scam's peak in FYs 2019 through 2021 (see Figure 2 below). Annually, Social Security-related scam reports have decreased significantly since FY 2021, and according to the Federal Trade Commission (FTC), imposter scam complaints across the government have declined since 2021. However, Social Security-related scams remain a top government imposter type reported to the FTC.¹ Therefore, while the decline is promising, SSA OIG and SSA continue to fight these scams.

Figure 2

Long-term SSA-related Imposter Scam Allegations April 2018 to March 2025









1. This information is based on data reported to the FTC as of April 24, 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

Q1 and Q2 FY 2025 Complaint Trends – Percentage of Total Imposter Allegations from the Scam Reporting Form

Complaint Characteristics		Q1 10/1/24–12/31/24	Q2 1/1/25–3/31/25
	The imposter mentioned a problem with your Social Security number	25.8%	17.4%
	The imposter mentioned a problem with your Social Security benefits	17.4%	18.0%
	The imposter used documents or images (such as a federal logo) when communicating with you	27.9%	23.3%
	The scam involved the impersonation of officials from federal, state, or local government agencies other than the Social Security Administration	33.6%	36.1%
	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	2.5%	3.7%
	None of the Above	42.3%	49.4%

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 Q1 FY 2025, slightly fewer individuals 50 years of age or older reported financial losses than those under 50 years of age. Figure 4 (below) shows that in Q2 FY 2025, this trend changed. In Q2 FY 2025, 320 individuals under 50 years of age reported losses, compared with 337 individuals 50 years of age and older.

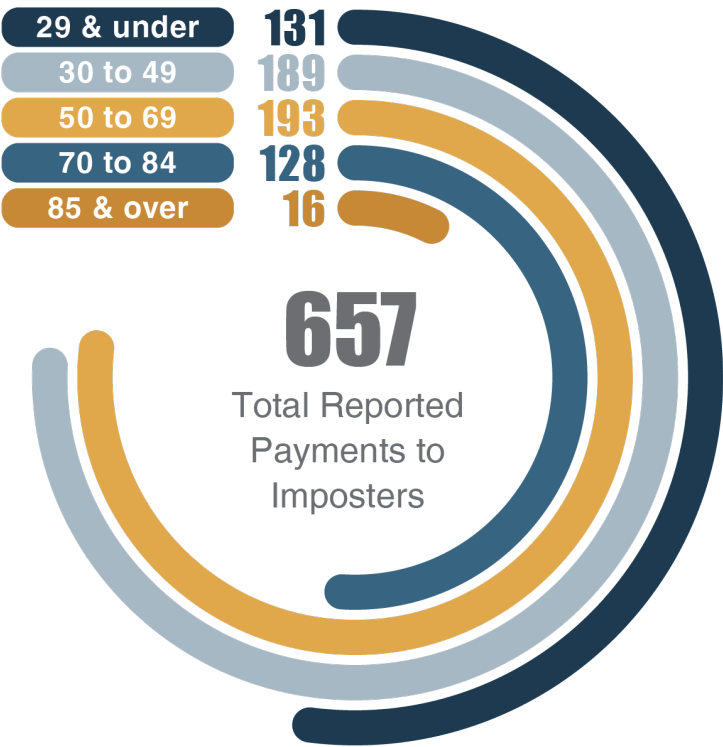
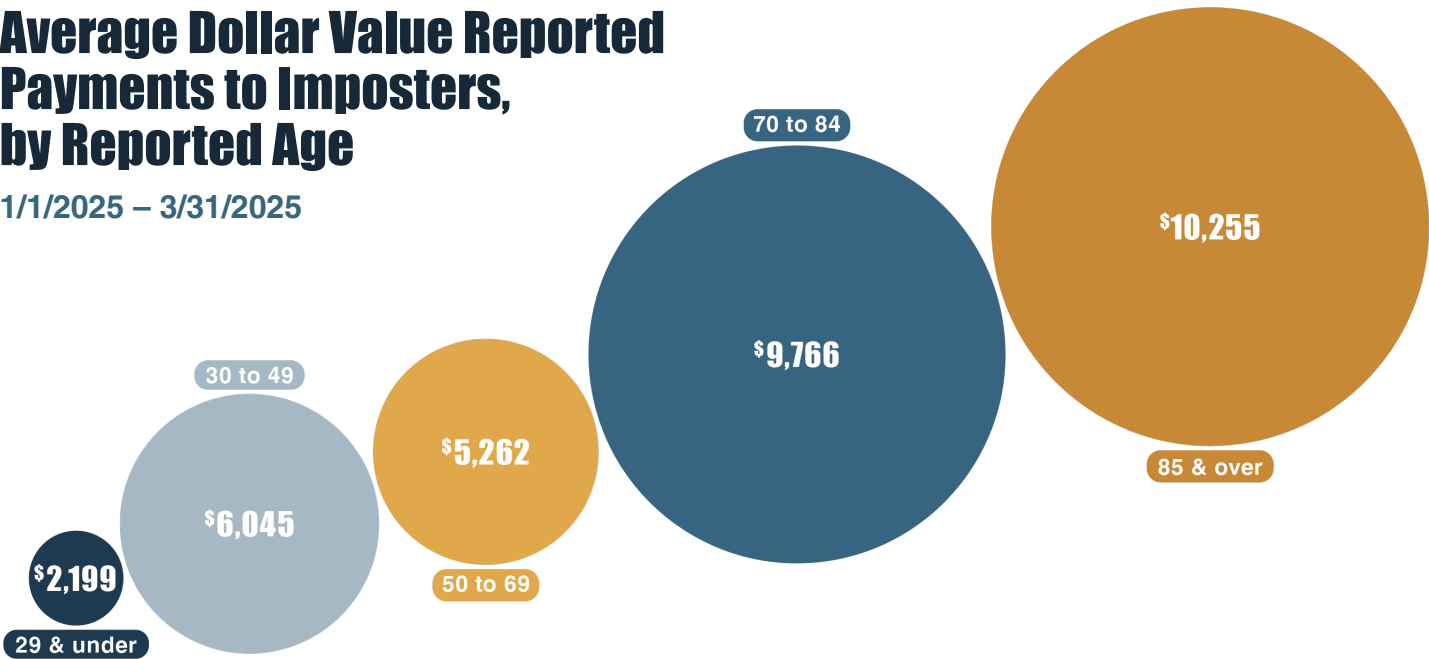


Figure 4
Number of Reported Payments to Imposters, by Reported Age
1/1/2025 – 3/31/2025

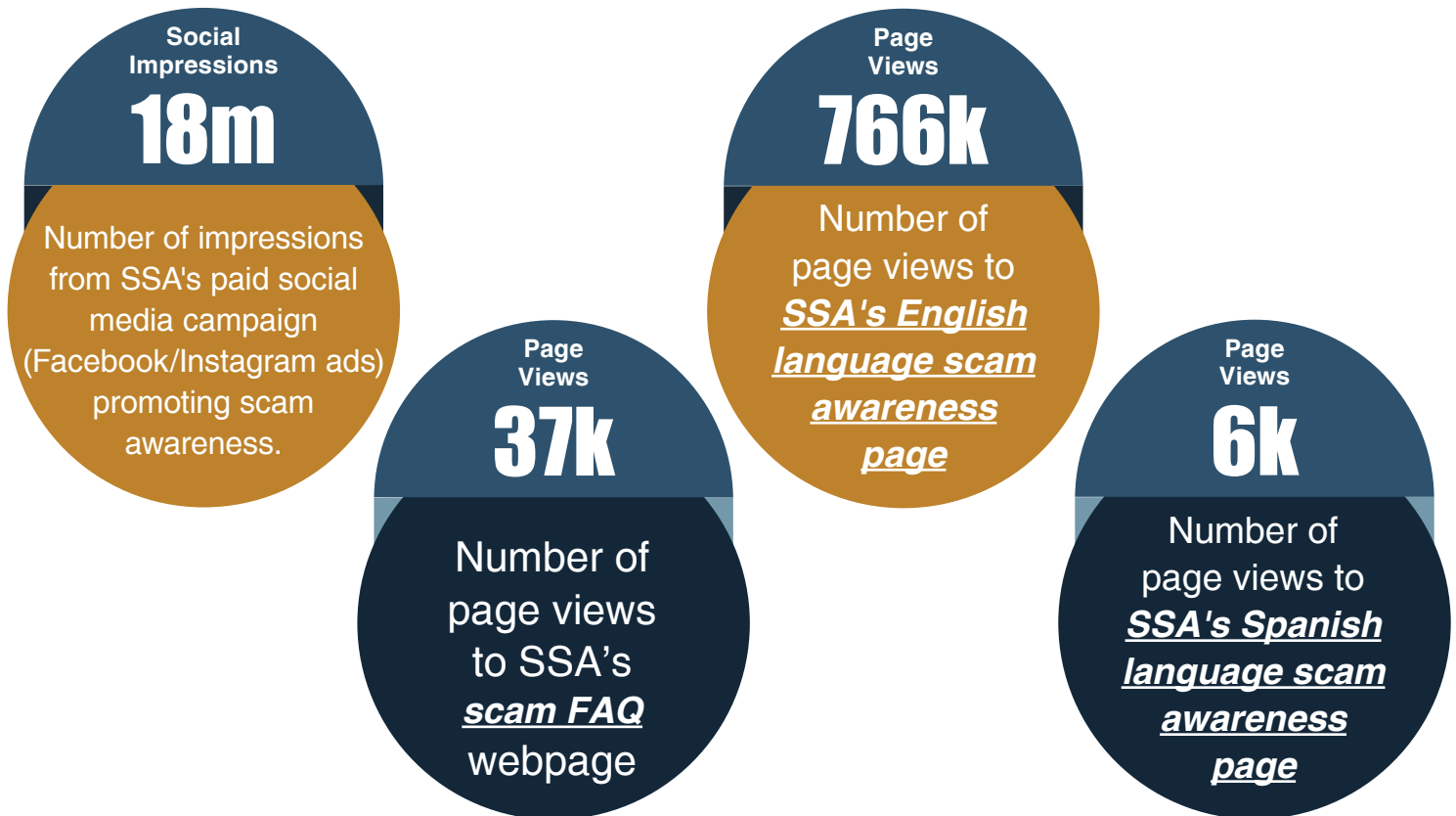
In Q1 FY 2025, individuals 70 years of age and over reported higher average losses than those under 70 years of age. Figure 5 (below) shows that in Q2 FY 2025, this trend continued.

Figure 5
Average Dollar Value Reported Payments to Imposters, by Reported Age
1/1/2025 – 3/31/2025



Q2 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 **7.4 million page views**. Website page views, clicks, and social media impressions for Q2 FY 2025 are shown below.



In Q2 FY 2025, SSA mailed **97 million** letters to the public with a scam alert message on the back of envelopes (right). The Agency has mailed almost **1.4 billion** of these letters to date.

⚠ SCAM ALERT ⚠

Scammers are pretending to be government employees. They may threaten you and may demand immediate payment to avoid arrest or other legal action. Do not be fooled!

If you receive a suspicious call:

1. HANG UP!
2. DO NOT GIVE THEM MONEY OR PERSONAL INFORMATION!
3. REPORT THE SCAM AT [OIG.SSA.GOV](https://oig.ssa.gov)



SSA's October 2021 *Scam Awareness Public Service Announcement* [video](#) (left) generated **2.4 million** impressions in Q2 FY 2025.



SSA's November 2023 [video](#) (left), *How to Spot a Scam*, garnered **5,489** views in Q2 FY 2025.

The Spanish language version of the video, *Cómo detectar una estafa*, had **1,524** views during Q2 FY 2025.

Q2 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 Q2 FY 2025 included the activities below.



Throughout January 2025, SSA displayed slides on Identity Theft Awareness Week and Cost-of-Living Adjustment scams to monitors in its field and hearing offices.

On January 2, 2025, SSA published a blog titled, [Resolve to Protect Yourself From Scams This Year](#), which provided information about protecting social media profiles, being savvy with QR codes, using strong passwords, and being cautious when sharing personal information.



On January 30, 2025, SSA [partnered with the FTC for webinars](#) in English and Spanish to help the public better understand, avoid, and recover from identity theft.

Throughout February 2025, SSA displayed a Tax Season scam awareness slide on monitors in its field and hearing offices.



On February 13, 2025, SSA published a blog titled, [7 Ways Veterans Can Protect Themselves From Scams](#), to warn about scammers posing as employees of the Veterans Administration who contact veterans by phone, mail, email, and social media and offer to help them access or file for benefits on their behalf – for a fee.

In March 2025, SSA and SSA OIG developed an internal process to ensure timely distribution of new scam alerts to frontline employees.



On March 26, 2025, SSA OIG presented on Section 1140 of the *Social Security Act* at the National Association of Disability Representatives (NADR) annual conference, highlighting various types of SSA-related scams and fraud schemes. NADR is an organization of attorney and non-attorney disability advocates.

Throughout Q2 FY 2025, SSA OIG met with agencies across the federal government to amplify scam awareness messages and collaborate on initiatives to protect Americans from scams and fraud.



Throughout Q2 FY 2025, SSA OIG and SSA engaged in internal awareness and external outreach activities related to National Slam the Scam Day. See page 7 for more details.

On March 6, 2025, SSA OIG partnered with SSA for the sixth annual National Slam the Scam Day. As part of the FTC's National Consumer Protection Week, Slam the Scam Day raises public awareness of the pervasive Social Security-related and other government imposter scams. This year SSA and SSA OIG engaged in outreach with media, Congressional, intragovernmental, and other stakeholders, and spread their message on social media.

National Slam the Scam Day

March 6, 2025



X (formerly Twitter)

18.4 Million

#SlamtheScam chats

Senate Resolution

Senate passed by
Unanimous Consent
S.Res.118 designating
March 6, 2025 as
**National Slam the
Scam Day**



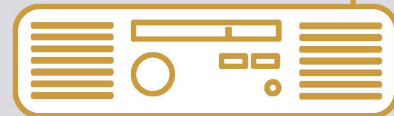
Facebook

6.9 Million

#SlamtheScam followers

Radio Audience:

234,000



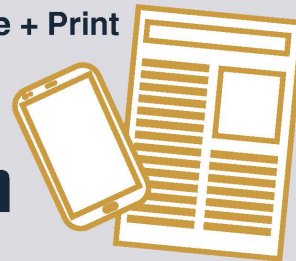
Instagram

47,000

reach from Slam the Scam posts

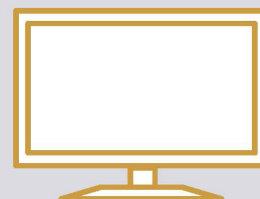
Total Online + Print
Audience:

**282
million**



Television Audience:

744,000



Note: All figures in this graphic are estimates.

March 2025 | Produced at U.S. taxpayer expense.

During Q2 FY 2025, SSA OIG issued three Scam Alerts. First, on February 11, 2025, SSA OIG issued **Do Not Click the Link to Claim SSA Benefits!** to warn members of the public of a new scam tactic by criminals trying to lure potential retirement applicants to their site. This recent scam email appears to be from SSA and has the subject line: “Claim Benefits!” It states “Important: Apply for Your Social Security Benefits Starting in 2025.” The link within the phony email is disguised as SSA’s official website, www.ssa.gov or www.socialsecurity.gov. Clicking on the link within the email redirects individuals to a fraudulent site.



Next, on February 26, 2025, SSA OIG issued **It's a New Scam: The Security Update Tool** cautioning the public to be aware of emails that appear to be from SSA and include a link to download a utility tool. This email is an attempt to lure individuals to fraudulent sites that are not associated with SSA by claiming there is a problem, or a potential error, and to correct the issue you must download a “Security Update Tool.” The email suggests the “Social Security monitoring system has identified a potential error” and recommends that you open, download and install a tool to your computer or device. However, this tool is not from SSA and will compromise personal data.

Finally, on March 19, 2025, SSA OIG issued **Don't Hand Off Your Assets for "Safe Keeping"** to warn the public of alarming reports of criminals impersonating SSA OIG agents and other federal law enforcement officials and requesting that their targets meet them in person to hand off cash, gold, or other forms of non-traceable currency. In some situations, scammers are providing copies of fraudulent government identification badges, which look genuine and may have names of actual government employees. Federal law enforcement officers will never text or email photographs of credentials or badges to prove their identity, and neither will federal employees.



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 Q2 FY 2025, SSA OIG:



Redeveloped and launched a domain name registration initiative whereby SSA OIG educates owners of recently acquired SSA-related domain names about Section 1140's prohibitions so the owners can avoid potential internet-related violations.

Renewed efforts to address SSA-related scam calls by utilizing vendor-supplied AI-equipped software to identify new targets suspected of engaging in SSA robocalling campaigns to unsuspecting Americans.



Met with SSA Regional Communications Directors and Public Affairs Specialists in an information session meant to equip frontline workers with prevention strategies against the latest trends in SSA-related social media scams.

Presented to provide NADR's members information to help educate their clients about scams and avoid violating Section 1140 in their advertising.



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.

Initiated five takedown requests and opened numerous inquiries regarding SSA-related imposter social media accounts and other communications.





OIG.SSA.GOV