



QUARTERLY SCAM UPDATE

Issue 18

OFFICE OF THE INSPECTOR GENERAL SOCIAL SECURITY ADMINISTRATION

July 1, 2025 – September 30, 2025

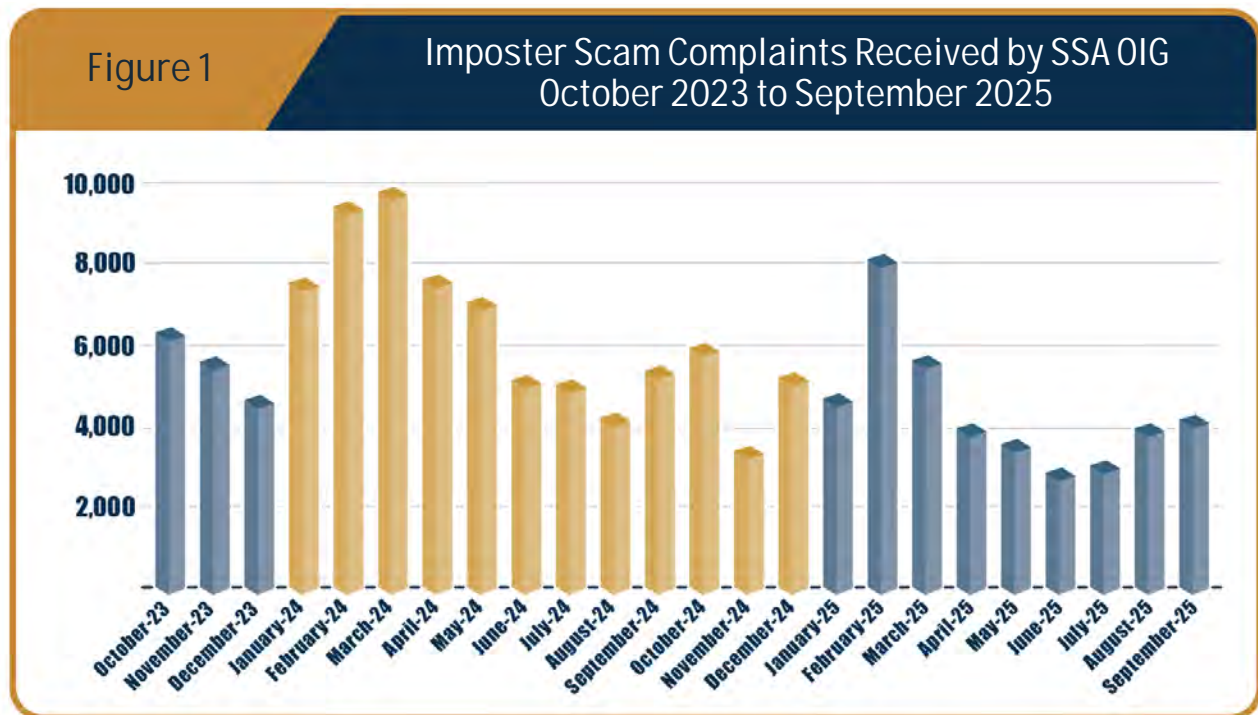
Social Security-Related Scams

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.

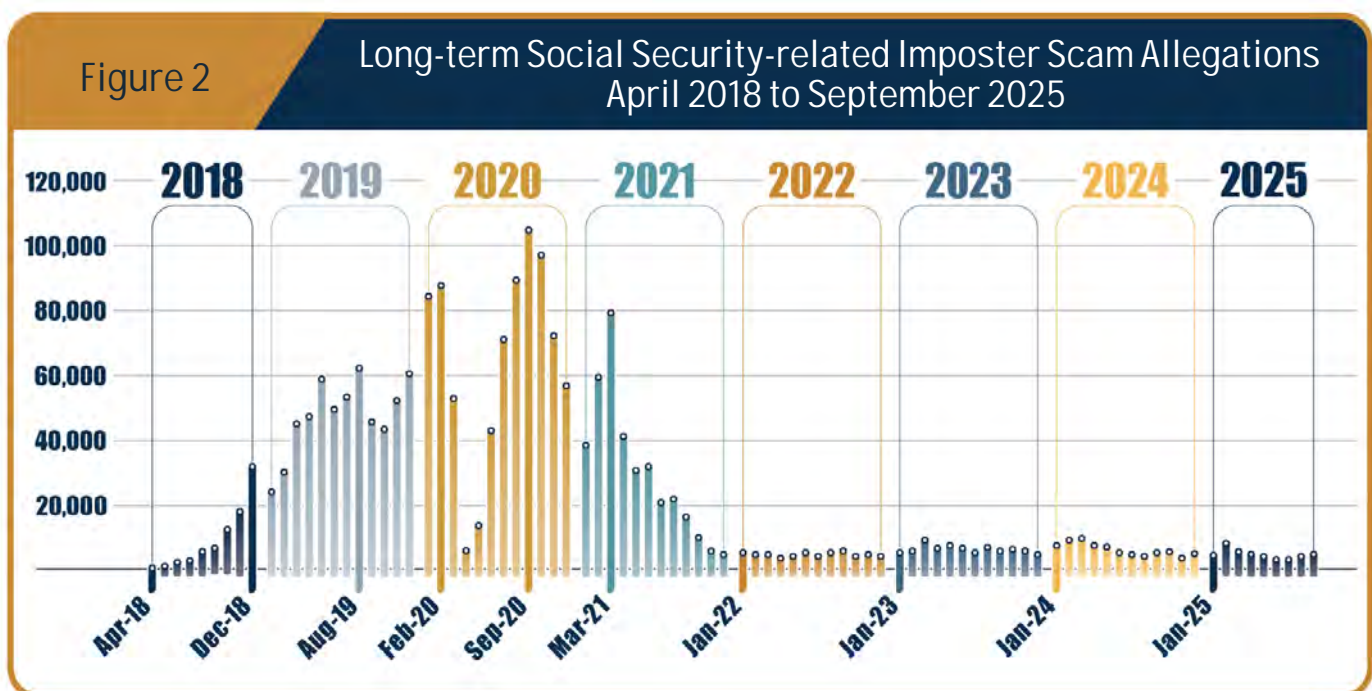
Since October 2019, SSA OIG has shared information on its efforts to combat Social Security-related scams with the U.S. House of Representatives Committee on Ways and Means, Subcommittee on Social Security; U.S. Senate Committee on Finance; and U.S. Senate Special Committee on Aging. SSA OIG began publicly 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 fourth quarter (Q4) of FY 2025 (July 1 through September 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 showed 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.¹ 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. The form is made available for individuals to report they received a suspicious call, letter, text, or email about an alleged problem related to their Social Security number, account, or payments. The form also allows individuals to report whether the scam involved impersonation of SSA, SSA OIG, or other government officials, along with other characteristics.

Figure 3

Q3 and Q4 FY 2025 Complaint Trends – Percentage of Total Allegations from the Scam Reporting Form

Complaint Characteristics		Q3 4/1/25–6/30/25	Q4 7/1/25–9/30/25
	The imposter mentioned a problem with your Social Security number	19%	19%
	The imposter mentioned a problem with your Social Security benefits	19%	12%
	The scammer mentioned a problem with your mySSA account or Social Security direct deposit information	N/A	90%
	The imposter used documents or images (such as a federal logo) when communicating with you	29%	25%
	The scammer pretended to be from the Social Security Administration or Office of the Inspector General	N/A	90%
	The scam involved the impersonation of officials from federal, state, or local government agencies other than the Social Security Administration	31%	17%
	The scammer requested your Social Security number or other personal information	N/A	90%
	None of the Above	40%	27%

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 Q4 FY 2025, SSA OIG enhanced the Scam Reporting Form to capture additional information about scam allegations. In this figure "N/A" is used to indicate that, because of this modification, the data is not available for three complaint characteristics in prior reporting periods.

In Q3 FY 2025, fewer individuals 50 years of age or older reported financial losses than those under 50 years of age. Figure 4 (below) shows that in Q4 FY 2025, this trend continued. In Q4 FY 2025, 404 individuals under 50 years of age reported losses, compared with 267 individuals 50 years of age and older.

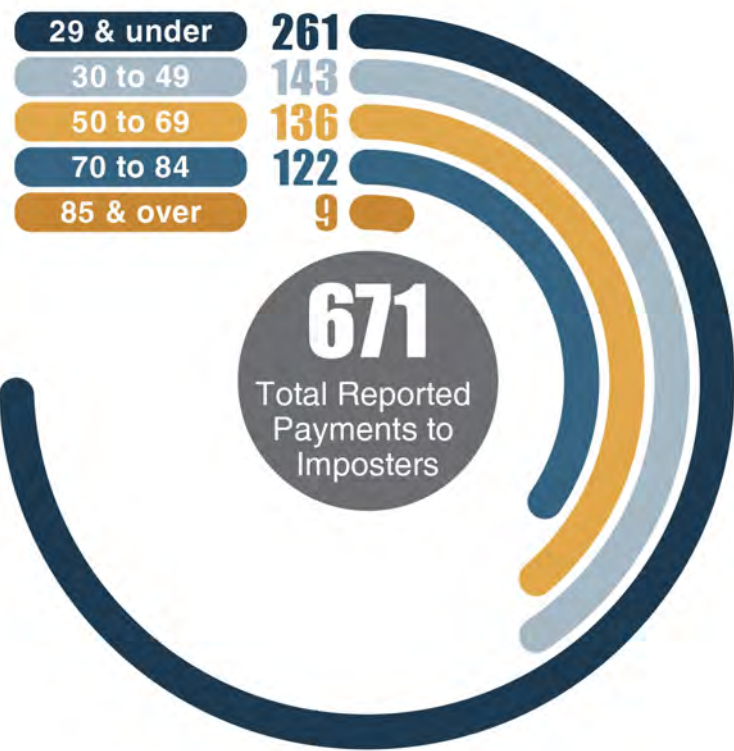


Figure 4
Number of Reported Payments to Imposters, by Reported Age
7/1/2025 – 9/30/2025

In Q3 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 Q4 FY 2025, this trend continued.

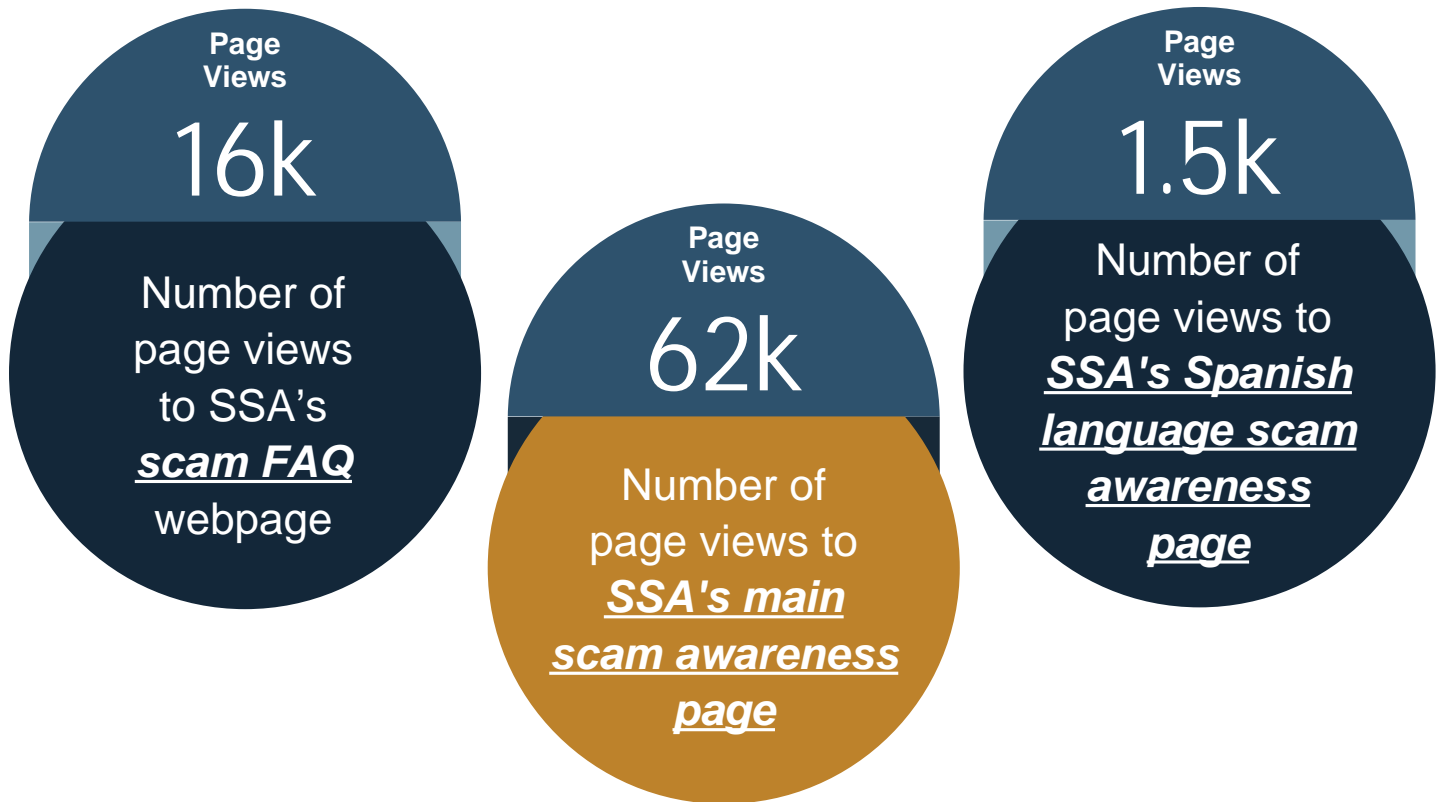


Figure 5
Average Dollar Value Reported Payments to Imposters, by Reported Age
7/1/2025 – 9/30/2025



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 **8.2 million page views**. Website page views, clicks, and social media impressions for Q4 FY 2025 are shown below.



Note: SSA experienced a loss of Google Analytics information related to page views during August 1 to September 4, 2025. The figures above are likely understated because of this data loss.



SSA's October 2021 *Scam Awareness Public Service Announcement* video (left) generated 960,000 impressions in Q4 FY 2025.

SSA's November 2023 video (right), *How to Spot a Scam*, garnered 1,536 views in Q4 FY 2025.

The Spanish language version of the video, *Cómo detectar una estafa*, had 1,466 views during Q4 FY 2025.



Q4 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 Q4 FY 2025 included the activities below.



In July 2025, SSA OIG participated in military consumer awareness month by posting on social media and sharing information with members of anti-scam workgroups.

On August 21, 2025, SSA OIG participated in an interview for WTHR 13 Investigates (Indianapolis) entitled 'I felt like I was victimized twice': Retired police officer warns Social Security of fraud, agency sends check to scammer anyway.



In August 2025, SSA OIG updated its website to include a scam warning banner advising the public about government imposter scams.

In September 2025, SSA OIG created a back-to-school scam awareness campaign, including posting important scam information on social media and sharing content with other agencies to encourage their participation. Follow SSA OIG on Facebook, X, and LinkedIn to keep up with the latest scam information.



Throughout Q4 FY 2025, SSA continued showing multiple scam awareness slides on televisions in its offices to remind visitors to remain vigilant against scams, including:

Protect Yourself From Social Security Scams

Social Security will **not**:

- Threaten you.
- Tell you there is a problem with or suspend your Social Security number.
- Demand an immediate payment from you.
- Require payment by retail gift card, pre-paid debit card, internet currency, wire transfer, or by mailing cash.
- Text or email images of an employee's badge.



During Q4 FY 2025, SSA OIG issued one Scam Alert. On July 31, 2025, SSA OIG issued **Unexpected Call or Message? Think Scam First** to warn the public to be aware of scammers pretending to be with SSA or the U.S. Department of Justice (DOJ), Office for Victims of Crime (OVC).

SSA OIG and OVC are advising the public to watch out for government imposter scams. Neither SSA nor OVC will demand money from you or threaten you with legal or criminal action if you do not pay. Government officials and law enforcement agents will never pick up money at your door or in any type of exchange. For example, scammers may represent themselves as SSA OIG agents and request that you meet them in person to hand off cash.

Key Warning Signs of a Scam

- Unexpected communication by phone call, text or social media message, email, or letter in the mail warning of a problem or offering a prize.
- Pressure in the form of threats, demands, or limited time offers.
- Payment requests of cash, gift cards, gold bars, prepaid debit cards, wire or money transfer, and cryptocurrency.

How to Protect Yourself

- Stop. Think scam. Talk to someone you trust before paying.
- Visit ssa.gov/scam to report Social Security-related scams and learn more.
- Stay up to date on the latest scam warnings and tactics by following SSA OIG on [X](#), [Facebook](#), and [LinkedIn](#).
- Visit the [Federal Trade Commission](https://www.ftc.gov) for consumer protection tips.

SCAM ALERT

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

FOR IMMEDIATE RELEASE
July 31, 2025

**Unexpected Call or Message?
Think Scam First**

Beware of scammers pretending to be with the **Social Security Administration (SSA)** or the **U.S. Department of Justice (DOJ), Office for Victims of Crime (OVC)**.

Stay skeptical and think **scam** anytime you get an unexpected or unsolicited call, message, or letter. The SSA Office of the Inspector General (OIG) and **OVC** are advising the public to watch out for government imposter scams. Neither SSA nor OVC will demand money from you or threaten you with legal or criminal action if you do not pay. **Government officials and law enforcement agents will never pick up money at your door or in any type of exchange.** For example, scammers may represent themselves as SSA OIG agents and request that you meet them in person to hand off cash.

"Scammers continue to exploit fear and confusion by impersonating trusted government agencies like SSA and OVC," said Michelle L. Anderson, Acting Inspector General for SSA. "We urge citizens to be vigilant, and to always question unexpected calls, texts, emails, or letters, and report suspected scams immediately."

Key Warning Signs of a Scam

- Unexpected communication by phone call, text or social media message, email, or letter in the mail warning of a problem or offering a prize.
- Pressure in the form of threats, demands, or limited time offers.
- Payment requests of cash, gift cards, gold bars, prepaid debit cards, wire or money transfer, and cryptocurrency.

How to Protect Yourself

- Stop. Think scam. Talk to someone you trust before paying.
- Visit ssa.gov/scam to report Social Security-related scams and learn more.
- Stay up to date on the latest scam warnings and tactics by following SSA OIG on [X](#), [Facebook](#), and [LinkedIn](#).
- Visit the [Federal Trade Commission](https://www.ftc.gov) for consumer protection tips.

These Are Scams!

- Claims that a law enforcement officer will pick up payment in person.
- Offers to "protect" your money by transferring it.
- Using the real name of an official listed on a government website.
- Official looking documents or pictures.
- Requests for personal information, such as your Social Security number.
- Threats to suspend your Social Security number or arrest you.
- Demand for secrecy.

Members of the press may make inquiries to Social Security OIG at oig.press@ssa.gov
Connect with us on social media: [X](#) [Facebook](#) [LinkedIn](#)

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 Q4 FY 2025, SSA OIG's efforts included:



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

Notifying a school district and a multinational corporation of potential network compromises regarding Social Security-related phishing email scams so that the entities could take proactive measures to combat future scams.



SSA OIG continued its vigilance in monitoring and responding to Social Security-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.



OIG.SSA.GOV

Office of the Inspector General

Quarterly Scam Update | Issue 18 | July 1, 2025 – September 30, 2025

Produced and published at U.S. taxpayer expense