



QUARTERLY SCAM UPDATE

Issue 10

OFFICE OF THE INSPECTOR GENERAL SOCIAL SECURITY ADMINISTRATION

July 1, 2023 – September 30, 2023

Social Security-Related Scams

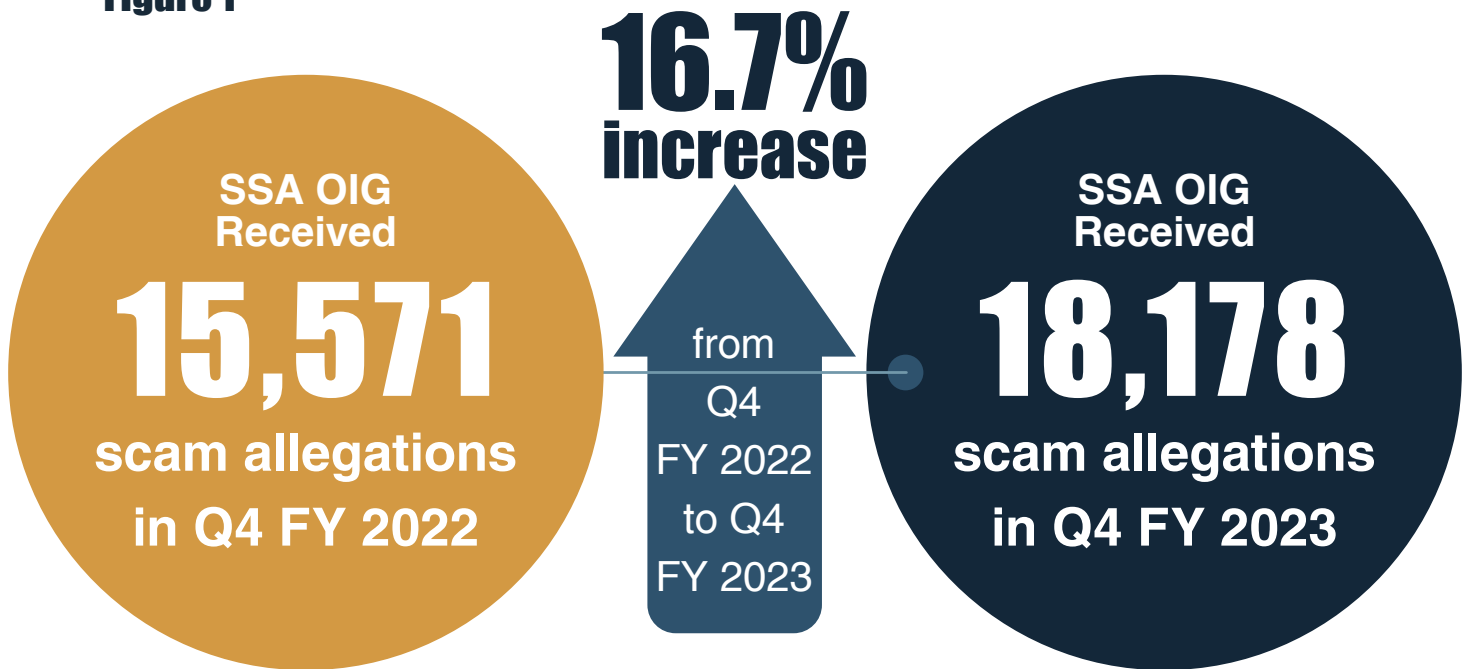
The Social Security Administration (SSA) and SSA Office of the Inspector General (OIG) continue to receive reports of scammers impersonating government employees or alleging a Social Security-related problem to steal money or personal information from victims.

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 and government imposter scam allegation trends in the fourth quarter (Q4) of FY 2023 (July 1 through September 30). Examples of SSA and SSA OIG's recent efforts to disrupt and raise awareness of scams are also included.



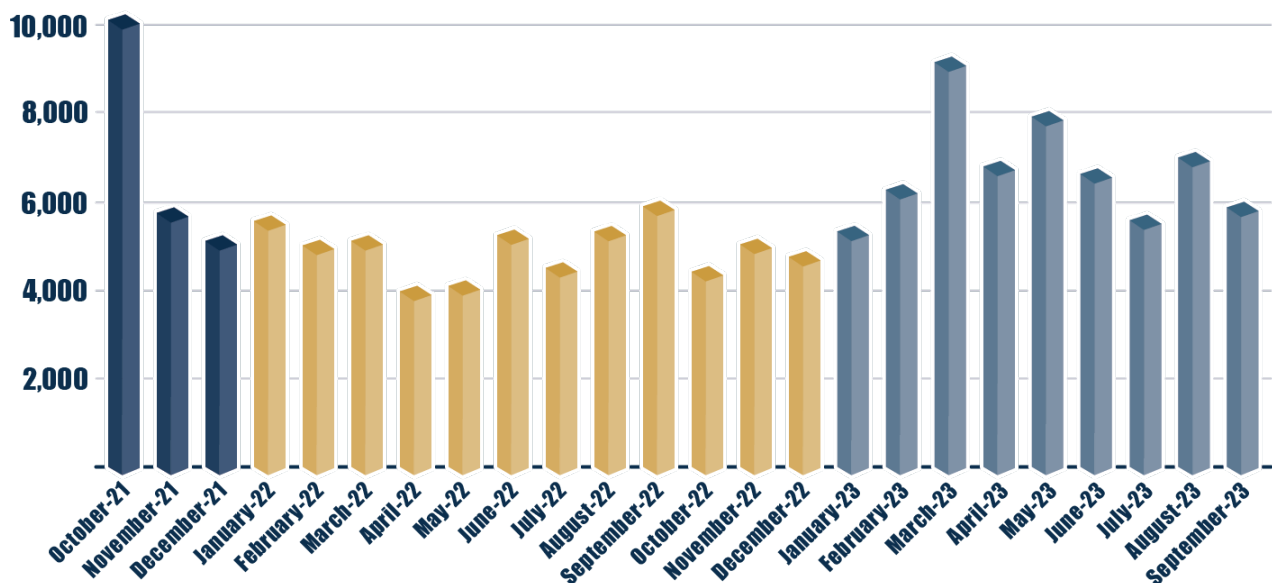
Figure 1



While scam allegations increased 16.7 percent from Q4 FY 2022 to Q4 FY 2023, scams reported to SSA OIG are still down significantly from Q4 in prior years. SSA OIG received 58,914 scam allegations in Q4 FY 2021, 265,169 in Q4 FY 2020 (during the scam's peak), and 161,376 in Q4 FY 2019. Following the sharp decline in FY 2021, SSA OIG has received fewer than 10,000 Social Security-related scam allegations per month from FY 2022 to the present.

Figure 2







Imposter Scam Complaints Received by SSA OIG
October 2021 to September 2023



SSA OIG receives the majority of Social Security-related scam allegations from its dedicated online scam reporting form. 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

Q3 and Q4 FY 2023 Complaint Trends – Percentage of Total Imposter Allegations from the Scam Reporting Form¹

Complaint Characteristics	Q3 4/1/23–6/30/23	Q4 7/1/23–9/30/23
 The imposter mentioned a problem with your Social Security number	45.0%	40.8%
 The imposter mentioned a problem with your Social Security benefits	15.5%	16.4%
 The imposter used documents or images (such as a federal logo) when communicating with you	30.7%	25.8%
 The scam involved the impersonation of officials from federal, state, or local government agencies other than the Social Security Administration	34.9%	37.3%
 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	2.1%	2.4%
 None of the Above	27.2%	28.5%

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.

1. These data also reflect allegations SSA OIG receives from other sources, including its Hotline and directly from SSA employees. SSA OIG has been tracking Social Security-related scam allegations since April 2018. SSA OIG launched the dedicated online reporting form in November 2019, which increased its ability to track scam reports.

In [Q3 FY 2023](#), slightly more individuals under 50 years of age reported financial losses than those 50 years of age or older. Figure 4 (below) shows that in Q4 FY 2023, this trend continued: 716 individuals under 50 years of age reported losses, compared with 675 individuals 50 years of age and older.

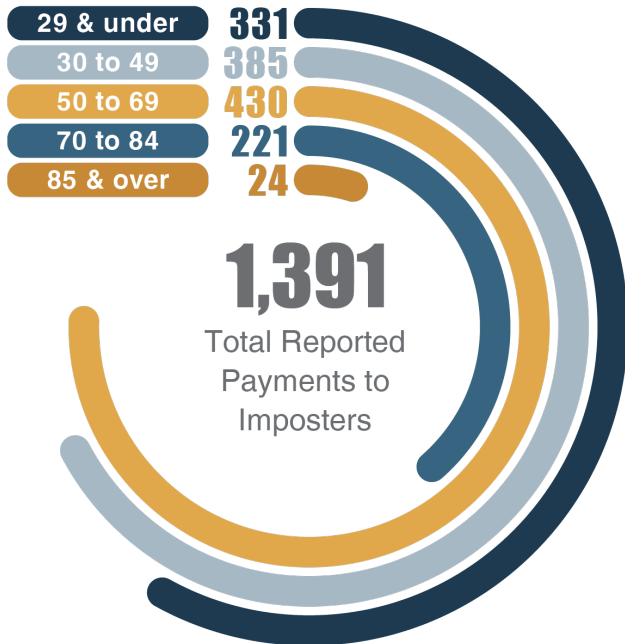


Figure 4

Number of Reported Payments to Imposters, by Reported Age

7/1/2023 – 9/30/2023

In [Q3 FY 2023](#), individuals 50 years of age and over reported higher average losses than those under 50 years of age. Additionally, during April 1 through June 30, 2023, the highest average losses were reported by individuals 85 years of age and over. Figure 5 (below) shows that in Q4 FY 2023, individuals 50 years of age and over continued to report higher average losses than those under 50 years of age. Additionally, during July 1 through September 30, 2023, the highest average losses were reported by individuals 70 to 84 years of age – slightly more than average losses reported by individuals 85 years of age and over.

Figure 5

Average Dollar Value Reported Payments to Imposters, by Reported Age

7/1/2023 – 9/30/2023

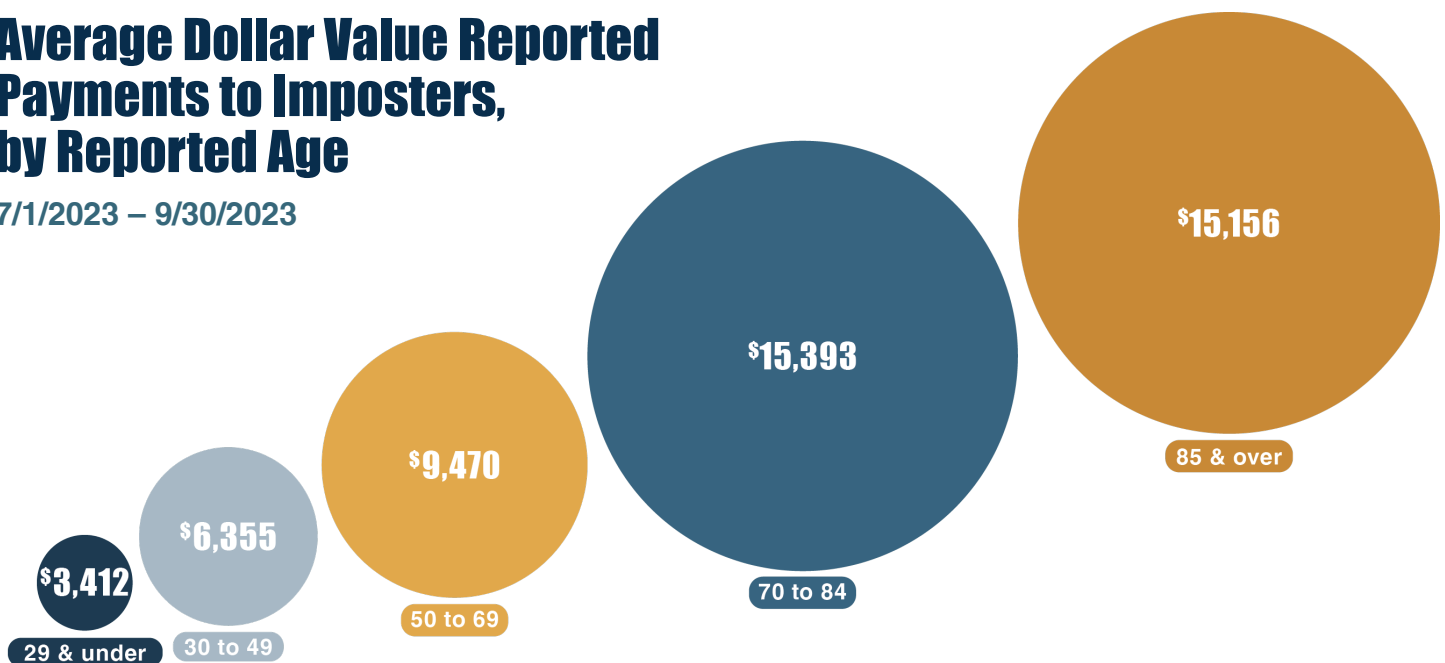
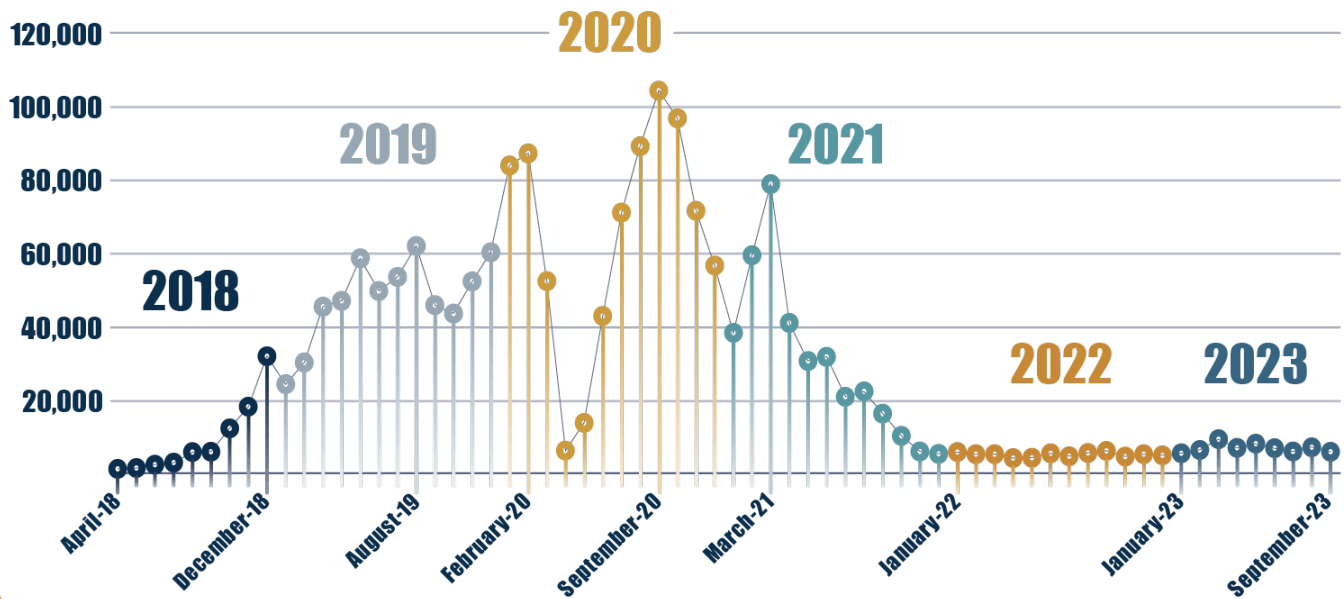


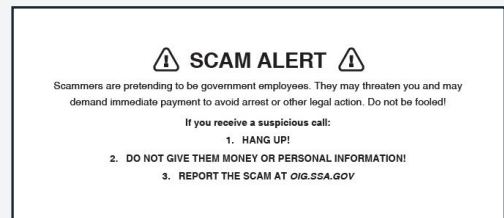
Figure 6

Long-term SSA-related Imposter Scam Allegations
April 2018 to September 2023



Annually, Social Security-related scam reports have decreased significantly since FY 2021, and according to the Federal Trade Commission (FTC), government imposter scam complaints have declined since 2021. However, Social Security-related scams remain the top government imposter type reported to the FTC.² Therefore, while the decline is promising, SSA OIG and SSA continue to fight these scams.

In Q4 FY 2023, SSA mailed 44.1 million letters to the public with a scam message printed on the back of envelopes (right). Through September 30, 2023, the Agency had mailed approximately **885.4 million** of these letters to date.



SSA's latest Scam Awareness Public Service Announcement (left), which started airing in late October 2021, generated 24.0 million impressions in Q4 FY 2023. The Public Service Announcement generated **313.2 million** total impressions during FY 2023.

2. This information is based on data reported to the FTC as of November 1, 2023.

Q4 FY 2023 Additional Internal and External Education Efforts

SSA and SSA OIG engaged in additional outreach and education efforts with members of the public, government and non-government organizations, and SSA employees to raise awareness of scams targeting American residents. Some examples of these efforts during Q4 FY 2023 included the activities below.



SSA and SSA OIG participated in a cross-component meeting with leadership from SSA's Office of Native American Partnerships to discuss ways to reach tribal communities with fraud and scam messaging.

SSA and SSA OIG met with the FTC to discuss best practices and strategies for reaching emerging readers and older adults with fraud and scam messaging.



SSA released two Video on Demand trainings to employees related to Identity Theft and Fraud and Social Media.

SSA OIG briefed members of the U.S. House of Representatives Committee on Ways and Means Subcommittee on Social Security on its response to Artificial Intelligence (AI)-assisted threats to programs and systems.



SSA OIG participated in an interview with Baltimore, Maryland television station WMAR-ABC on AI-enabled scams.

SSA and SSA OIG serve on committees with the FTC and other law enforcement partners as a result of the *Stop Senior Scams Act*, which established the Senior Scams Prevention Advisory Council.

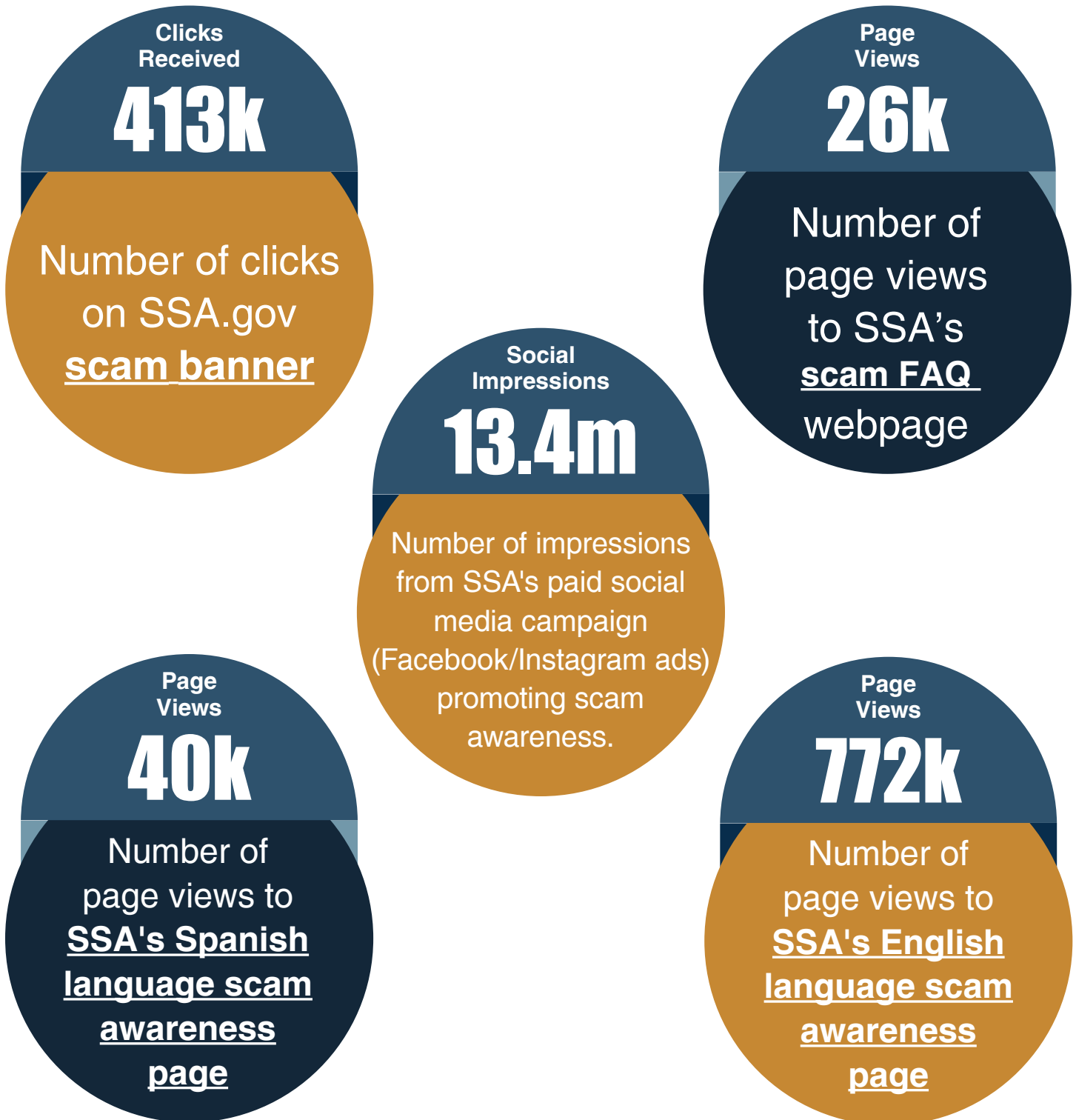


National Anti-fraud Committee Annual Summit Collaboration to Fight Fraud and Artificial Intelligence Scams

SSA and SSA OIG have a shared duty to the public to fight fraud in SSA's programs. In September 2023, SSA OIG and the Agency jointly held the third annual National Anti-Fraud Summit to understand and address fraud issues facing SSA, with an emphasis on AI-driven scams. The Summit featured a speaker from the Department of Energy OIG, who spoke about how AI is impacting modern fraud schemes and federal agency responses. Other topics included plans to protect SSA from AI-related scams, digital identity programs, consumer protection from government impersonation, fraud trends, and insider threats. The Summit led to additional collaboration between the OIG and the Agency.

Q4 FY 2023 Website Page Views and Social Media Impressions

An SSA and SSA OIG joint scam page redesign resulted in an increase in page views to the scam page. Since the launch of the redesign on May 19, 2022, there have been **2.47 million page views** of the scam page including **132,221 clicks** on the Report a Social Security-related Scam button and **104,593 clicks** on the Report a Scam button. Website page views, clicks, and social media impressions for Q4 FY 2023 are below.



Consumer Protection: Telephone and Social Media Scams

Section 1140 of the *Social Security Act*, as amended, protects the public from advertisements, solicitations, and other communications that convey the false impression that SSA approved, endorsed, or authorized the communication. SSA OIG continued efforts to protect consumers from Social Security-related scam calls originating outside of the U.S. by seeking corrective action against U.S. based telecommunications companies, acting as gateway carriers, who profit by accepting Social Security-related scam calls into the U.S. telecommunications system, and passing them to unsuspecting consumers. During Q4 FY 2023, SSA OIG resolved a matter with a gateway carrier, resulting in the imposition of a \$17,000 penalty. To date, SSA OIG has imposed penalties against 23 gateway carriers for their involvement with Social Security-related scam calls.

As a result of SSA OIG's Section 1140 and other efforts, the telecommunications industry is on notice of the potential legal ramifications for their involvement with Social Security-related scam calls. Telecommunications companies are continuing to take more proactive steps to prohibit scam calls from entering the U.S. or are discontinuing the gateway carrier segment of their operations or operations entirely.

In addition to SSA OIG's scam call efforts, SSA OIG continues to stay vigilant regarding Social Security-related imposter social media accounts. SSA OIG recognizes the public's vulnerability to harm from social media scams, as well as the negative impact these scams have on the Agency's ability to effectively communicate via its robust social media program. During Q4 FY 2023, SSA OIG continued its efforts of monitoring social media platforms for imposter accounts, initiated 3 take down requests for SSA-related imposter accounts and continued reviewing social media imposter account cases for potential civil monetary penalty action.

SSA OIG Partners with the Federal Trade Commission to Stop Illegal Telemarketing Calls to U.S. Consumers

In July 2023, the FTC and more than 100 federal and state law enforcement agencies nationwide, including SSA OIG, announced a new crackdown on illegal telemarketing calls involving more than 180 actions targeting operations responsible for billions of calls to U.S. consumers.

The joint federal and state initiative, "Operation Stop Scam Calls," is part of FTC's ongoing efforts to combat the scourge of illegal telemarketing, including robocalls. The initiative targets telemarketers and the companies that hire them and takes action against lead generators who deceptively collect and provide consumers' telephone numbers to robocallers and others, falsely representing that these consumers have consented to receive calls. The effort also targets Voice over Internet Protocol (VoIP) service providers who facilitate illegal robocalls, which often originate overseas.

In addition to FTC actions, 48 federal and 54 state agencies, including SSA OIG, have brought more than 180 enforcement actions and other initiatives as part of Operation Stop Scam Calls. In addition to SSA OIG, contributing law enforcement partners include the Department of Justice, which has announced several civil and criminal actions related to this initiative, the Federal Communications Commission, and the U.S. Postal Inspection Service.

You can read more about Operation Stop Scam Calls [here](#).

Man Sentenced in Connection with a \$1.5 Million Social Security-Related Imposter Scam

In August 2023, an Indiana man was sentenced for perpetuating a Social Security-related government imposter scam where he stole approximately \$1.5 million from individuals, including from older victims. The man's co-conspirators utilized call centers in India to contact victims in the U.S. and pretend to be government officials and law enforcement agents. They told victims their SSNs had been found in connection with criminal activity, often narcotics trafficking, and stated the victims would be arrested if they did not immediately withdraw large sums of cash and mail it to a fictitious individual via U.S. Mail, FedEx, or another commercial private carrier in Indiana. From April 2017 through April 1, 2021, the man tracked the packages of money sent by fraud victims to the fictitious recipients and picked them up at multiple FedEx locations. In each instance, he used a false identification document in the name of the listed package recipient. In total, he possessed at least 53 false identification documents, each with his picture but containing different identifying information. He used these false identification documents to pick up at least 122 packages containing \$901,124 in cash. He retained \$60,000 for his own use and forwarded the remainder of the cash to his associates. You can read more about the case [here](#) and in [SSA OIG's Fall 2023 Semiannual Report to Congress](#).

Leader of Identity Theft Conspiracy who Stole Nearly 50 Vehicles Sentenced to 8.5 Years in Prison

In September 2023, a Massachusetts man was sentenced in federal court for orchestrating schemes to use the stolen identities of U.S. citizens from Puerto Rico to fraudulently purchase vehicles and other merchandise and apply for and utilize bank accounts and credit cards. The man was sentenced to 102 months in prison and three years of supervised release. He was also ordered to pay \$389,141 in restitution to victims. He pleaded guilty to one count of conspiracy to commit wire fraud; two counts of wire fraud; three counts of aggravated identity theft; and three counts of false representation of a Social Security number in Massachusetts. He also pleaded guilty to a similar scheme in New Jersey, which was investigated by SSA OIG and transferred to the District of Massachusetts for resolution. Between October 2017 and September 2020, he was the leader of a conspiracy that used stolen identity information to obtain credit and goods. Under his direction, and with stolen identity information that he provided, co-conspirators visited car dealerships to purchase late-model vehicles and applied for 100% financing. In support of the applications, the co-conspirators provided stolen biographical information and Social Security cards as proof of identification. The co-conspirators used the stolen identities to illegally open bank accounts and credit cards and purchase vehicles. You can read more about the case [here](#).

Indian National Sentenced to 10 Years in Federal Prison for Money Laundering Conspiracy

In September 2023, an Indian National residing in Colorado was sentenced to 120 months of imprisonment, followed by deportation to India, for conspiring to commit money laundering. The judge also ordered restitution of \$1,163,947 to the victims. In January 2020, he began his involvement in a Social Security-related government imposter scam where victims were contacted by persons impersonating government officials from various federal agencies, including SSA. The imposters threatened victims with arrest or deportation unless they paid the government and also told victims their payments would be held in trust. Typically, the imposters told victims to immediately withdraw cash from their bank accounts and remain on the phone during the entire bank transaction. The imposters told the victims to mail packages of cash via FedEx locations, typically inside Walgreen's stores, or United Parcel Service stores. It was also found that two other runners were the Indian National's co-conspirators in the scheme. You can learn more about the case [here](#) and in [SSA OIG's Fall 2023 Semiannual Report to Congress](#).



OIG.SSA.GOV