QUARTERLY SCAM UPDATE
Issue 2

OFFICE OF THE INSPECTOR GENERAL
SOCIAL SECURITY ADMINISTRATION

JULY 1, 2021 – SEPTEMBER 30, 2021

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 our efforts to combat Social Security-related scams with the House Committee on Ways and Means, Social Security Subcommittee; Senate Committee on Finance; and Senate Special Committee on Aging. We began publicly releasing the *Quarterly Scam Update* last quarter to provide information about these scams and our efforts.

This report addresses trends in Social Security-related scam allegations, as well as our ongoing efforts to raise public awareness of, and disrupt the scams in the fourth quarter (Q4) of Fiscal Year (FY) 2021 (July 1 through September 30).

Volume of Social Security-Related Scam Allegations in Q4

OIG received fewer reports[1] of Social Security-related[2] scams during the 3 months of Q4 than any other quarter in FY 2021. In September 2021, we received approximately 16,000 scam allegations, just half of the volume in June 2021, the last month in the third quarter of 2021 (Q3). Our September volume of allegations also reflects an 85 percent decrease from September 2020, when we received approximately 105,000 scam allegations.

The following figures show the trends in two different formats, as well as general scam trends for the past 24 months.[3]

Figure 1 **Imposter Scam Complaints Received by SSA OIG (October 2019 to September 2021)**

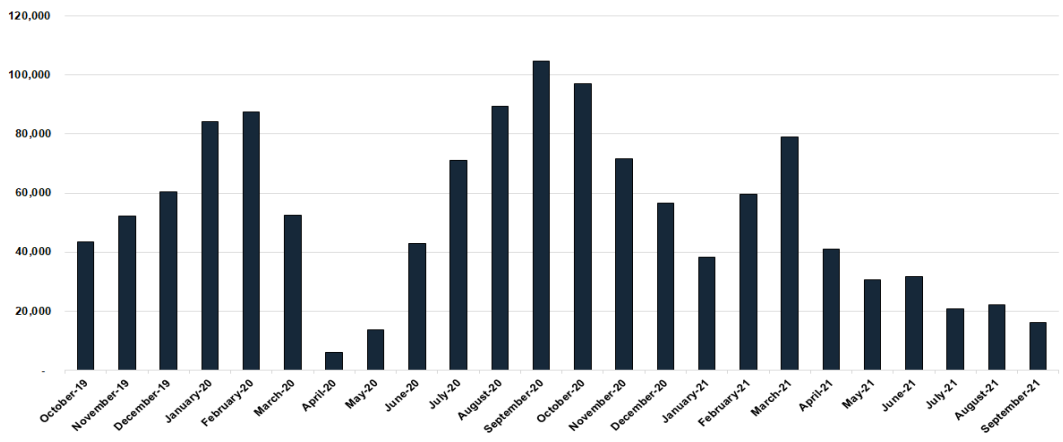
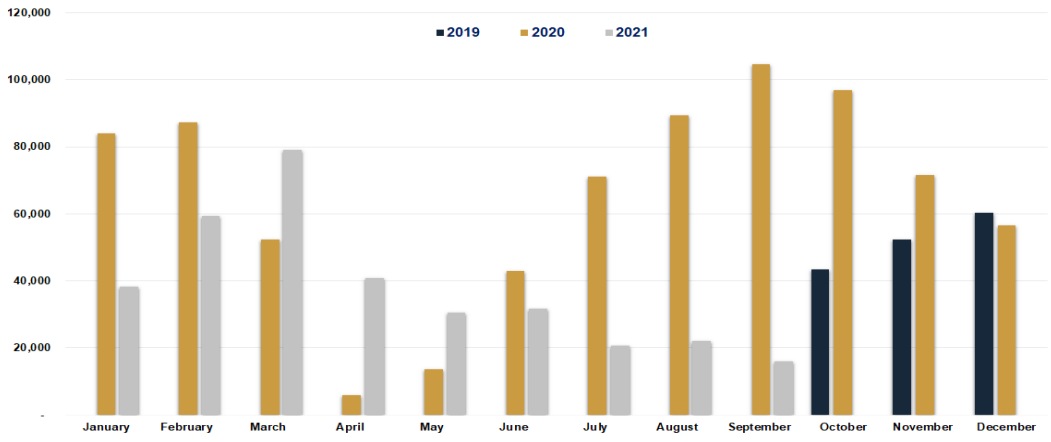


Figure 2 **Impersonation Scam Complaints Received by SSA OIG (October 2019 to September 2021)**



Date Prepared: October 15, 2021

[1] The number of Social Security-related scam allegations OIG receives may not reflect all Social Security-related scams. This is because the allegations are self-reported. For the same reason, allegations of financial losses to scammers may not reflect all alleged losses.

[2] These scams primarily use the telephone, but a small number of scams are reported to have been communicated via email, social media, text, or U.S. mail.

[3] We have been tracking Social Security-related scam allegations since April 2018. We launched the dedicated online reporting form in November 2019, which greatly increased our ability to track scam reports.

Sources of Information

We receive the majority of Social Security-related scam allegations from OIG's dedicated online scam reporting form.[4] Among other information, the form lists the following six characteristics of scams and asks complainants to check all that apply:

1) whether the imposter mentioned problems with the individual's Social Security number (SSN);
2) whether the imposter mentioned problems with the individual's Social Security benefits;
3) whether the imposter used documents or images (such as a federal logo) when communicating;
4) whether the scam involved the impersonation of officials from federal, state, or local government agencies other than the Social Security Administration;
5) whether 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; or
6) whether none of the above apply.

In addition to scam characteristics, the form asks the complainant's state of residence, age, whether the individual experienced a financial loss, the amount of the loss, and the method the imposter used to contact the individual, such as by telephone, email, or other means.

Trends in Allegations of Social Security-Related Scams

Table 1, below, compares how complainants responded to the six scam characteristics on the scam form for each quarter of FY 2021. The three most common characteristics in scam complaints were: 1) imposters mentioning problems with the complainant's SSN; 2) imposters impersonating government officials; and 3) imposters mentioning problems with the complainant's Social Security benefits. In FY 2021, 80.4 precent of complainants indicated that imposters mentioned problems with their SSN.

Table 1: FY 2021 Complaint Trends (Percentage of Total Imposter Allegations from the Scam Reporting Form)

Complaint Characteristics	Q1 10/1/20 – 12/31/20	Q2 1/1/21 – 3/31/21	Q3 4/1/21 – 6/30/21	Q4 7/1/21 – 9/30/21	FY 2021
The imposter mentioned a problem with your Social Security number	83.6%	81.1%	76.7%	72.7%	**80.4%**
The imposter mentioned a problem with your Social Security benefits	17.2%	17.9%	16.7%	14.9%	**17.1%**
The imposter used documents or images (such as a federal logo) when communicating with you	2.4%	2.8%	3.4%	5.2%	**3.0%**
The scam involved the impersonation of officials from federal, state, or local government agencies other than the Social Security Administration	34.7%	38.9%	41.1%	42.1%	**38.0%**
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	0.7%	1.0%	1.2%	1.6%	**1.0%**
None of the Above	5.4%	6.3%	8.0%	10.3%	**6.7%**

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.

[4] We also receive allegations from other sources, including OIG's Hotline and directly from SSA employees.

Loss Frequency and Amount by Age

As we previously reported, analysis of our scam reporting form shows more individuals under 50 reported instances of financial loss to scammers than those over 50. However, individuals over 50 reported losses that were higher than those under 50. Figures 3 and 4, below, break down these trends further for FY 2021. We note this analysis is based upon data from complainants who voluntarily self-reported both a date of birth and a dollar value loss. These trends continued in Q4, and the results are consistent with earlier trends reported by the Federal Trade Commission (and referenced in the Inspector General's January 2020 testimony on imposter scams before the Senate Special Committee on Aging).[5]

Figure 3 **Number of Reported Payments to Imposters, by Reported Age**
10/1/2020 - 9/30/2021

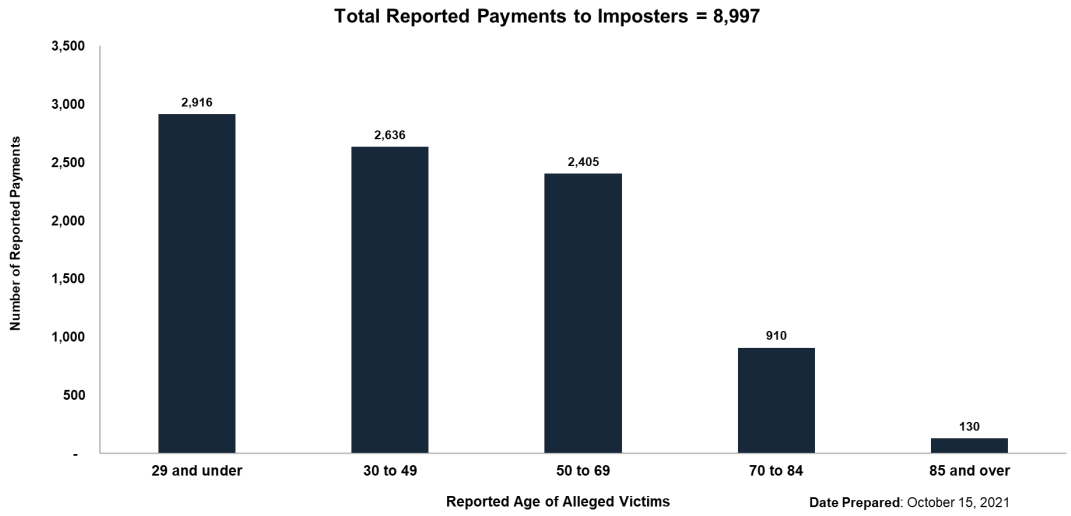
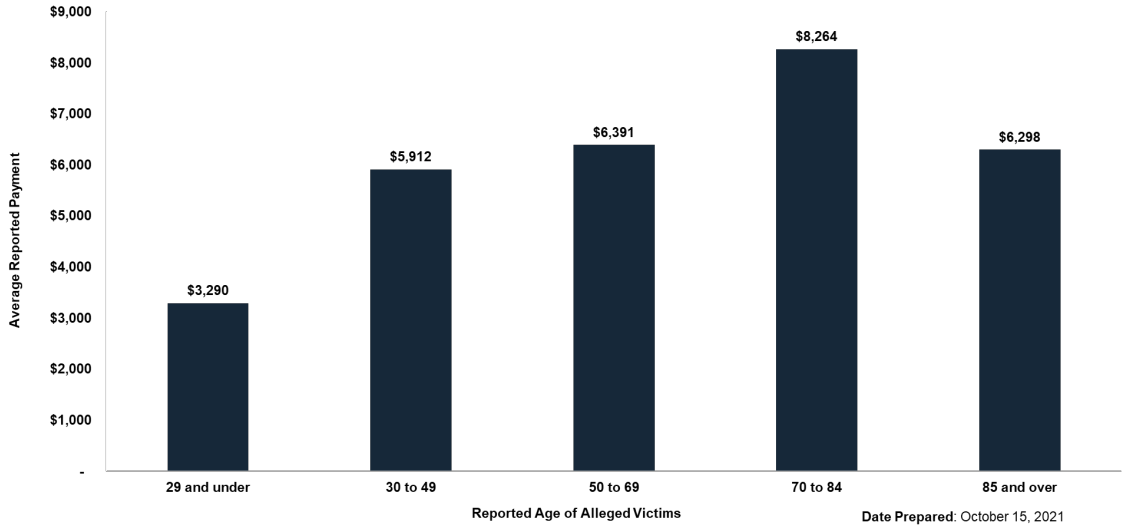


Figure 4 **Average Dollar Value of Reported Payments to Imposters, by Reported Age**
10/1/2020 - 9/30/2021



[5] Inspector General Ennis testified that according to the Federal Trade Commission (FTC), in Fiscal Year 2019, about 81 per 100,000 people ages 20-29 years old reported a fraud loss to the FTC due to government imposter scams. For those ages 80 years or older, the rate was about 40 per 100,000. However, the median fraud loss amount for those ages 20-29 was $1,000, while for ages 80 and over, it was $3,000.

Geographic Trends

Data from our scam reporting form also shows the number of complaints received from each state, and the average dollar value of the reported loss. However, allegations from our scam reporting form have dropped nearly 75 percent during FY 2021 and continued to decline throughout the first 2 months of FY 2022 (allegations totaled just 5,430 in November 2021). Therefore, we are not including any specific geographic trend information until we can further assess how such information may be provided in the context of the significant drop in overall reporting volume.

Fourth Quarter (FY 2021 – July 1, 2021 – September 30, 2021) Initiatives to Combat Social Security-related Scams

OIG combats Social Security-related scams by investigating scam allegations and engaging in public outreach to inform citizens how to recognize, respond to, and report scams. Below are some investigative and outreach highlights from this reporting period.

- **Investigation – Robocall Conspirators Confess:** On August 4, 2021, Zeeshan Khan and Maaz Ahmed Shamsi pleaded guilty to one charge each of conspiracy to commit wire fraud. As part of an international fraud scheme, call centers, believed to be in India, used automated robocalls with the intent of defrauding thousands of U.S. residents, particularly the elderly. Callers claimed they were from a U.S. government or law enforcement agency such as SSA, the Internal Revenue Service, or the Federal Bureau of Investigation (FBI). They used various schemes to coerce victims into sending cash through physical shipments or wire transfers to other members of the conspiracy, including Shamsi and Khan. Shamsi and Khan were charged with receiving an aggregate $618,000 in fraudulent wire transfers from 19 victims across the country. The victims paid these fraudsters between $5,000 and $58,540 each. Shamsi and Khan face up to 20 years in prison and a $250,000 fine or twice the amount of the loss, whichever is greatest. You can read more about this case here.

- **Investigation – Runner Pleads Guilty:** On September 13, 2021, Waseem Maknojiya pled guilty to conspiracy to commit mail fraud. Between April and October 2019, Maknojiya acted as a runner in a telemarketing scheme via Indian call centers to extort money from victims in the United States, using aliases and fake identification documents to retrieve more than 70 parcels containing cash the scheme's victims had mailed. One common script used in the scheme involved coercing victims into believing federal agents from SSA, FBI, or the U.S. Drug Enforcement Administration were investigating them. The "agent" on the phone would convince the victim the only way to clear his or her name from investigation was to send cash in a parcel shipped to a name and address they provided. Maknojiya would then pick up the parcels. As part of his plea agreement, Maknojiya will pay restitution to the scheme's identified victims. Maknojiya faces up to 20 years in prison and a possible $250,000 maximum fine. He will remain in custody pending that hearing. You can read more about this case here.

- **Social Media Campaign to Recognize Retail Employees Who Intervene to Prevent Fraud:** Scammers frequently demand payment in the form of retail gift cards, which are easily accessible and difficult to trace. Retail workers selling these gift cards are often the last line of defense against scammers. In August, we highlighted one such "scam fighter" on our Facebook and Twitter accounts. This individual, a Target store employee in Rochester, New York, intervened to stop a scam. Specifically, the employee noticed a customer trying to make thousands of dollars in gift card purchases. The employee remembered her training on government imposter scams and suspected the customer was a victim of a Social Security-related scam. The employee urged the customer not to purchase the gifts cards and to call police. This intervention saved the customer from losing thousands of dollars in this scam.

OIG presented the employee with a certificate of appreciation, as shown in the pictures below.

- **Public Service Announcement:** SSA and OIG developed new public service announcements on Social Security-related scams and shared them on social media and with media outlets. Watch the new PSA here.

- **Thieves Don't Take a Vacation Campaign:** We worked with SSA to develop a post for Social Security Matters (SSA's blog), Twitter, and Facebook reminding the public that thieves do not take a vacation from trying to scam people, and urging individuals to stay vigilant year round.

- **Presentation on Scams at Various Conferences:** OIG presented information on Social Security-related scams to various organizations and advocacy groups.

- **Elder Awareness Organizations:** In September 2021, as part of OIG's strategy to address pervasive Social Security-related scams and to increase our reach, we connected with special interest groups, including the American Association of Retired Persons, Legal Advocates for Seniors and People with Disabilities, National Center for Elder Abuse, National Hispanic Council on Aging, National Indian Council on Aging, SAGE–Advocacy & Services for LGBT Elders, and Women's Institute for Secure Retirement. We shared a flyer with these groups, providing scam information to help their members protect themselves from Social Security-related scams.

- **SSA's Public Mailings:** In Q4 of FY 2021, SSA mailed 35 million letters to the public, with a fraud message printed on the back of all envelopes. Through September 2021, the Agency has mailed approximately 328 million of these letters in total

Please contact us with any questions: oig.dcom@ssa.gov

Follow us on social media:
Twitter: @TheSSAOIG • Facebook: OIGSSA • YouTube: TheSSAOIG

OIG.SSA.GOV