Consumer Protection Data Spotlight
FTC reporting back to you

Growing wave of Social Security imposters overtakes IRS scam

Claiming to be a government authority is a tried and true way that scammers trick people into sending money. Among the most common government imposters have been scammers pretending to be the IRS – until now. In the past few months, the FTC's Consumer Sentinel Network database has seen Social Security Administration (SSA) imposter reports skyrocket while reports of IRS imposters have declined sharply. In the shady world of government imposters, the SSA scam may be the new IRS scam.

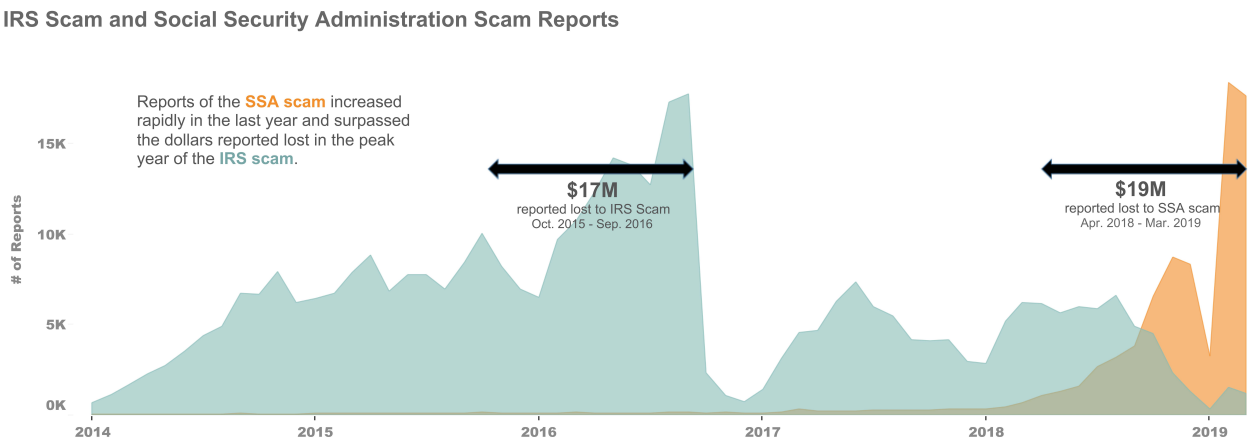
SSA imposters tell you your Social Security number has been suspended because of suspicious activity, or because it's been involved in a crime. They ask you to confirm your Social Security number, or they may say you need to withdraw money from the bank and to store it on gift cards or in other unusual ways for "safekeeping." You may be told your accounts will be seized or frozen if you don't act quickly.

These scammers often use robocalls to reach people, and the message can be hard to ignore. You may be told to "press 1" to speak to a government "support representative" for help reactivating your Social Security number. They also use caller ID spoofing to make it look like the Social Security Administration really is calling. With such trickery, these scammers are good at convincing people to give up their Social Security numbers and other personal information.

As the graphic shows, people reported the IRS scam (in blue) in huge numbers for many years, but the new SSA scam (in orange) is trending in the same direction – with a vengeance. People filed over 76,000 reports about Social Security imposters in the past 12 months, with reported losses of $19 million.[1] Compare that to the $17 million in reported losses to the IRS scam in its peak year.[2] About 36,000 reports and $6.7 million in reported losses are from the past two months alone.

Just 3.4% of people who report the Social Security scam tell us they lost money.[3] Most people we hear from are just worried because they believe a scammer has their Social Security number. But when people do lose money, they lose a lot: the median individual reported loss last year was $1,500, four times higher than the median individual loss for all frauds.[4] All age groups are reporting this scam in high numbers, with older and younger adults filing loss reports at similar rates.[5]

People report sending money in unconventional ways.



Most often, people say they gave the scammer the PIN numbers on the back of gift cards. Virtual currencies like Bitcoin come in a distant second to gift cards: people say they withdrew money and fed cash into Bitcoin ATMs. With both methods, the scammer gets quick cash while staying anonymous, and the money people thought they were keeping safe is simply gone.

Here are some tips to deal with these imposters:

- **Do not trust caller ID**. Scam calls may show up on caller ID as the Social Security Administration and look like the agency's real number.
- **Don't give the caller your Social Security number or other personal information.** If you already did, visit IdentityTheft.gov/SSA to find out what steps you can take to protect your credit and your identity.
- **Check with the real Social Security Administration.** The SSA will not contact you out of the blue. But you can call them directly at 1-800-772-1213 to find out if SSA is really trying to reach you and why.
- **Talk about it.** People recognize the IRS scam, but many are getting caught off guard by these new imposters. You can help by telling people that the SSA scam is a new version of the IRS scam.

Report government imposter scams to the FTC at FTC.gov/complaint. To learn more, visit ftc.gov/imposters.

1 The FTC was unable to collect reports directly from the public during the government shutdown. Reports collected during that period were provided by Sentinel data contributors.

2 From October 1, 2015 to September 30, 2016, about 140,000 reports of IRS imposter scams were filed and collectively indicated $17 million of loss.

3 For comparison, 2.8% of IRS scam reports filed from January 2014 through March 2019 indicated a loss. In 2018, 25% of all fraud reports indicated a loss.

4 Median loss calculations are based on reports submitted in 2018 that indicated a monetary loss ($1 - $999,999). The median reported individual loss to all frauds was $371 in 2018.

5 Age comparison based on the number of Social Security imposter reports that indicated a monetary loss per million population by age. People who said they were 20 – 59 filed loss reports at a rate of 8.9 reports per million people in this age group, while people who said they were 60 and over filed 10.0 loss reports per million people in this age group. Population numbers obtained from the U.S. Census Bureau: U.S. Census Bureau, Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States, States, Counties and Puerto Rico Commonwealth and Municipios (June 2018). Not all reports include usable age information.

The FTC uses reports from the public to investigate and stop fraud, for consumer education and outreach, and for analyses like this. File your fraud report at FTC.gov/complaint. To explore Sentinel data, visit FTC.gov/data.