Here's How a Growing Social Security Impostor Scam Works

To scammers, your Social Security number is gold-plated and diamond-encrusted asset, and now they have a new way to try to steal yours and get paid.

Consumer advocates are raising an alert about a twist to an old impostor phone scam. It's called the "Social Security impostor scam." A blog at the Federal Trade Commission recently wrote: "In the shady world of government, the SSA scam may be the new IRS scam."

Here's how it works:

You get a call with a warning that your Social Security number has been suspended because of suspicious activity or because it's been used in a crime. You are asked to confirm your number or told you need to withdraw money from the bank and buy gift cards.

The phone call may be a robocaller with a message to "press 1" to speak with a "support representative" from the government to reactivate your Social Security number. The scammers use technology to spoof your Caller ID to make it look like the Social Security Administration is really calling.

In the last 12 months, people filed more than 76,000 complaints about Social Security impostors, reporting $19 million in losses. The median reported loss last year was $1,500, the FTC said.

People are asked to give up the personal identification numbers (PINs) on the back of gift cards or use virtual currencies like Bitcoin to pay. (According to the FTC's consumer alert, people withdrew money and fed cash into Bitcoin automatic teller machines.)

After handing over the gift card numbers to the "Social Security office," one consumer interviewed by Fraud.org was told he would receive a refund equal to the amount he paid to unfreeze his account from the Federal

Reserve. Of course, the refund never came and the man lost nearly $20,000.

"One scammer will try a new twist on an old scam or try one new wrinkle that gets them more money," said John Breyault, vice president of public policy, telecommunications and fraud with the National Consumers League. "Scammers like to keep up with the Joneses when it comes to using the latest techniques to defraud consumers."

The scammers can be clever. With numerous data breaches that have hit corporate America, fraudsters may already have accurate personal information about you, including your real Social Security number, Breyault said. The information is used to build trust and make the call seem more legitimate, he added.

According to Fraud.org and the FTC, here are some important things to remember:

- Don't trust your phone's caller ID. Scammers can make it look as if the Social Security Administration is calling and even use the agency's real number.
- Don't give your Social Security number, other personal information, to a caller on the phone.
- Social Security will never suspend your number, according to Fraud.org. If anyone tells you something different, you're being scammed.
- Social Security will never call you and demand money. No government agency will demand you pay something using gift cards or Bitcoin either.
- If you have a question, check with the real Social Security Administration. The administration will never contact you out of the blue. The agency's number is 1-800-772-1213.
- Talk about the scam with friends, family and neighbors. Report government impostor scams to the FTC

By David Willis