Hackers steal even more Social Security numbers. How should you protect yourself?

23 August 2021, by Jon Healey

Credit: Pixabay/CC0 Public Domain

Another day, another massive data breach claimed by hackers. Days after a breach at T-Mobile exposed about 53 million people's personal information, a hacking group known as ShinyHunters announced that it was auctioning 70 million sets of sensitive data purportedly stolen from AT&T.

The information offered for sale was similar in both breaches, including full names, addresses, birth dates and Social Security numbers. In short, it's the foundation for identity theft.

AT&T responded Friday by casting doubt about the claim by the prolific ShinyHunters cabal, stating that "based on our investigation today, the information that appeared in an internet chat room does not appear to have come from our systems."

Regardless of where the data came from, though, if it's valid it could be a nightmare for anyone whose sensitive information is exposed. Here's a quick guide to the risks you may face and some of the things you can do to protect yourself.

What are the risks?

Social Security numbers are widely used by the federal government, banks, investment companies, government benefit programs and insurers to verify your identity. Your stolen Social Security number can be used to open fraudulent credit card accounts, divert or fraudulently collect benefits and commit workplace fraud, among other forms of deceit. Throw in your name, birth date and email address (which the ShinyHunters claim to have stolen too), and it's significantly easier for someone to pretend to be you.

Identity thieves could use that information to target both you and the banks, insurers and other companies you do business with. For example, they could use it to make phishing emails seem more realistic, helping to persuade you to give up additional sensitive information such as a password or personal identification number (PIN). Or they could use it to dupe your bank into letting them change the password on your account, giving them access to your money.

The T-Mobile breach also exposed the phone numbers, device identifiers and SIM-card numbers for more than 13 million of its current customers. That creates an opening for at least one more malign possibility: a SIM-swap attack. That's where someone persuades your mobile phone company to transfer your number to a different device, which he or she then uses to try to break into the accounts that you've tied to your phone number.

It's increasingly common for people to use their mobile phone numbers as a way to verify their identity—for example, when they log into their online banking account, or when they want to reset their password. But that convenience can backfire if your number is hijacked, then used to impersonate you online.

Why do phone companies want your Social

Security number?

Because it's the easiest way to check your credit rating. Companies like AT&T and T-Mobile want to know if you have a record of paying your bills on time before agreeing to provide you an account or to sell you a phone in monthly installments. And the major credit rating agencies use Social Security numbers to match people to their credit histories.

"The SSN is the only unique universal identifier across the entire population," explained Francis Creighton of the Consumer Data Industry Association, which represents the credit agencies. "There's nothing else that can replace it in today's market."

Social Security numbers also help guard against people setting up fraudulent credit reports, Creighton said. And while there are ways to establish a credit score that don't rely on your Social Security number, he said, the first step is for a lender or service provider not to ask for it. You can't be compelled by a phone company or other private-sector business to reveal your number, but in California and most other states, the business can refuse to serve you as a result.

Once you've paid off your new phone or switched carriers, though, your mobile company will no longer be filing reports about you to the credit bureaus, Creighton said. Nevertheless, the hackers behind the latest T-Mobile breach were able to steal Social Security numbers for former T-Mobile customers that the company held onto for some reason.

For the last decade, tech companies have been developing alternative ways of identifying people to make it easier to guard against identify theft, said André Ferraz, chief executive of Incognia, one of those tech companies. Ideally, Ferraz said, companies would supplement identifiers that cannot be changed, such as Social Security numbers, with identifiers based on a person's unique behaviors, which evolve over time. Unfortunately, those solutions haven't been widely adopted yet.

How do you protect yourself?

The single best thing to do is to put a freeze on your credit files, which will prevent anyone from opening a new account. It's free to place a freeze and to lift it for your own needs. But you have to contact each of the three major credit bureaus individually, which you can do online. Cybersecurity expert Brian Krebs also suggests freezing the credit files maintained by a handful of smaller, specialized agencies. You should also check your credit score regularly, which is a good way to detect fraud after it happens.

Credit- and identity-monitoring services, which typically carry a monthly fee, can also help reveal the work of identity thieves. They provide tools to prevent you from phishing and other forms of hacking combined with scanning services that look for your Social Security number or email address in places online where it doesn't belong.

T-Mobile is offering two years of McAfee's monitoring service for free to anyone affected by the breach. It has set up a website suggesting more steps people can take to guard against fraud. Anyone with a smartphone would be wise to take them:

- Create a PIN for your mobile phone account to provide an extra layer of security against unauthorized changes in your account, such as a malicious SIM swap. If you're a T-Mobile customer and you have a PIN, set a new one.
- Activate T-Mobile's "account takeover protection" feature, which provides an extra layer of protection on top of the PIN. Verizon goes further, automatically blocking SIM swaps by shutting down both the new device and the existing one until the account holder weighs in with the existing device.
- Change the password you use to get into your mobile phone account online. Changing passwords periodically is a good practice for all your accounts. And if you have trouble remembering dozens of passwords, try a password manager app that can keep track of them for you.

On the plus side, two-factor authentication is

becoming the standard online, and that's improving security across the web. But too many sites encourage you to make that second factor a text message sent to your phone number, which encourages SIM swap fraud. Wherever possible, use an authentication app instead.