Hackers stole millions of Social Security numbers from T-Mobile. What should you do?

August 19 2021, by Jon Healey, Los Angeles Times

Credit: CC0 Public Domain

Hackers have found their way again into T-Mobile's systems, the fourth reported breach of the company's data since early 2020. This time, the

haul included sensitive personal information associated with about 48 million people, most of whom were former or prospective customers of the self-styled "un-carrier."

Here is a breakdown of what happened, the risks you might face and how you can protect yourself against them.

What information was taken?

According to the company, the stolen data included names, birth dates, Social Security numbers and driver's license information. In most cases, the company said, "no phone numbers, account numbers, [personal identification numbers], passwords, or financial information were compromised." However, some 850,000 customers with prepaid accounts had their names, phone numbers and account PINs exposed, T-Mobile revealed.

Hackers started offering the data for sale last weekend, according to security researcher Brian Krebs, who predicted that it would all wind up online soon.

Although the potential number of people affected is huge, by T-Mobile's count it represents less than half the company's current 105 million customers. T-Mobile has said it will notify the customers whose data was exposed and provide two years of identity theft protection service for free from the security company McAfee.

What are the risks?

There have been so many data breaches at so many companies over the years, some security experts say that much of the information exposed by T-Mobile is probably already available on the dark web. But that

doesn't mean you should just shrug off what happened. Those whose data were exposed face greater risks of identity theft, phishing scams and other forms of fraud, Krebs warned.

Social Security numbers are widely used by the federal government, banks, investment companies, government benefit programs and insurers to verify identity. Your stolen SSN 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 driver's license number, and it's exponentially 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 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.

For those whose phone numbers were also exposed, there's 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 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.

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. 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.

Meanwhile, T-Mobile 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 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 make that second factor a text to your phone number, which encourages SIM swap fraud. Wherever possible, use an authentication app instead.