Los Angeles Times

BUSINESS

Hackers may have stolen the Social Security numbers of every American. Here's how to protect yourself

The breach, which includes Social Security numbers and other sensitive data, could power a raft of identity theft, one expert says. (Jenny Kane / Associated Press)

By Jon Healey
Deputy Editor, Fast Break Desk

Aug. 13, 2024 3 AM PT

About four months after a notorious hacking group claimed to have stolen an extraordinary amount of sensitive personal information from a major data broker, a

member of the group has reportedly released most of it for free on an online marketplace for stolen personal data.

The breach, which includes Social Security numbers and other sensitive data, could power a raft of identity theft, fraud and other crimes, said Teresa Murray, consumer watchdog director for the U.S. Public Interest Research Group.

For the record:

2:39 p.m. Aug. 15, 2024 *A previous version of this article identified Teresa Murray as the consumer watchdog director for the U.S. Public Information Research Group. She works for the U.S. Public Interest Research Group.*

"If this in fact is pretty much the whole dossier on all of us, it certainly is much more concerning" than prior breaches, Murray said in an interview. "And if people weren't taking precautions in the past, which they should have been doing, this should be a five-alarm wake-up call for them."

According to a class-action lawsuit filed in U.S. District Court in Fort Lauderdale, Fla., the hacking group USDoD claimed in April to have stolen personal records of 2.9 billion people from National Public Data, which offers personal information to employers, private investigators, staffing agencies and others doing background checks. The group offered in a forum for hackers to sell the data, which included records from the United States, Canada and the United Kingdom, for $3.5 million, a cybersecurity expert said in a post on X.

The lawsuit was reported by Bloomberg Law.

Last week, a purported member of USDoD identified only as Felice told the hacking forum that they were offering "the full NPD database," according to a screenshot taken by BleepingComputer. The information consists of about 2.7 billion records, each of

which includes a person's full name, address, date of birth, Social Security number and phone number, along with alternate names and birth dates, Felice claimed.

BUSINESS

Data of nearly all AT&T customers downloaded in security breach

July 12, 2024

National Public Data didn't respond to a request for comment, nor has it formally notified people about the alleged breach. It has, however, been telling people who contacted it via email that "we are aware of certain third-party claims about consumer data and are investigating these issues."

In that email, the company also said that it had "purged the entire database, as a whole, of any and all entries, essentially opting everyone out." As a result, it said, it has deleted any "non-public personal information" about people, although it added, "We may be required to retain certain records to comply with legal obligations."

Several news outlets that focus on cybersecurity have looked at portions of the data Felice offered and said they appear to be real people's actual information. If the leaked material is what it's claimed to be, here are some of the risks posed and the steps you can take to protect yourself.

The threat of ID theft

The leak purports to provide much of the information that banks, insurance companies and service providers seek when creating accounts — and when granting a request to change the password on an existing account.

A few key pieces appeared to be missing from the hackers' haul. One is email addresses, which many people use to log on to services. Another is driver's license or passport

photos, which some governmental agencies rely on to verify identities.

Still, Murray of PIRG said that bad actors could do "all kinds of things" with the leaked information, the most worrisome probably being to try to take over someone's accounts — including those associated with their bank, investments, insurance policies and email. With your name, Social Security number, date of birth and mailing address, a fraudster could create fake accounts in your name or try to talk someone into resetting the password on one of your existing accounts.

"For somebody who's really suave at it," Murray said, "the possibilities are really endless."

It's also possible that criminals could use information from previous data breaches to add email addresses to the data from the reported National Public Data leak. Armed with all that, Murray said, "you can cause all kinds of chaos, commit all kinds of crimes, steal all kinds of money."

CALIFORNIA

Phishing attack hits L.A. County public health agency, jeopardizing 200,000-plus residents' personal info

June 14, 2024

How to protect yourself

Data breaches have been so common over the years, some security experts say sensitive information about you is almost certainly available in the dark corners of the internet. And there are a lot of people capable of finding it; VPNRanks, a website that rates virtual private network services, estimates that 5 million people a day will access the dark web through the anonymizing TOR browser, although only a portion of them will be up to no good.

If you suspect that your Social Security number or other important identifying information about you has been leaked, experts say you should put a freeze on your credit files at the three major credit bureaus, Experian, Equifax and TransUnion. You can do so for free, and it will prevent criminals from taking out loans, signing up for credit cards and opening financial accounts under your name. The catch is that you'll need to remember to lift the freeze temporarily if you are obtaining or applying for something that requires a credit check.

TECHNOLOGY AND THE INTERNET

Are you the victim of identity theft? Here's what to do

Oct. 26, 2022

Placing a freeze can be done online or by phone, working with each credit bureau individually. PIRG cautions never to do so in response to an unsolicited email or text purporting to be from one of the credit agencies — such a message is probably the work of a scammer trying to dupe you into revealing sensitive personal information.

For more details, check out PIRG's step-by-step guide to credit freezes.

You can also sign up for a service that monitors your accounts and the dark web to guard against identity theft, typically for a fee. If your data is exposed in a breach, the company whose network was breached will often provide one of these services for free for a year or more.

If you want to know whether you have something to worry about, multiple websites and service providers such as Google and Experian can scan the dark web for your information to see whether it's out there. But those aren't specific to the reported National Public Data breach. For that information, try a free tool from the cybersecurity company Pentester that offers to search for your information in the breached National Public Data files. Along with the search results, Pentester displays links to the sites where you can freeze your credit reports.

As important as these steps are to stop people from opening new accounts in your name, they aren't much help protecting your existing accounts. Oddly enough, those accounts are especially vulnerable to identity thieves if you haven't signed up for online access to them, Murray said — that's because it's easier for thieves to create a login and password while pretending to be you than it is for them to crack your existing login and password.

WORLD & NATION

Trump campaign says its emails were hacked

Aug. 10, 2024

Of course, having strong passwords that are different for every service and changed periodically helps. Password manager apps offer a simple way to create and keep track of passwords by storing them in the cloud, essentially requiring you to remember one master password instead of dozens of long and unpronounceable ones. These are available both for free (such as Apple's iCloud Keychain) and for a fee.

Beyond that, experts say it's extremely important to sign up for two-factor authentication. That adds another layer of security on top of your login and password. The second factor is usually something sent or linked to your phone, such as a text message; a more secure approach is to use an authenticator app, which will keep you secure even if your phone number is hijacked by scammers.

Yes, scammers can hijack your phone number through techniques called SIM swaps and port-out fraud, causing more identity-theft nightmares. To protect you on that front, AT&T allows you to create a passcode restricting access to your account; T-Mobile offers optional protection against your phone number being switched to a new device, and Verizon automatically blocks SIM swaps by shutting down both the new device and the existing one until the account holder weighs in with the existing device.

Your worst enemy may be you

As much or more than hacked data, scammers also rely on people to reveal sensitive information about themselves. One common tactic is to pose as your bank, employer, phone company or other service provider with whom you've done business and then try to hook you with a text or email message.

Banks, for example, routinely tell customers that they will not ask for their account information by phone. Nevertheless, scammers have coaxed victims into providing their account numbers, logins and passwords by posing as bank security officers trying to stop an unauthorized withdrawal or some other supposedly urgent threat.

People may even get an official-looking email purportedly from National Public Data, offering to help them deal with the reported leak, Murray said. "It's not going to be NPD trying to help. It's going to be some bad guy overseas" trying to con them out of sensitive information, she said.

It's a good rule of thumb never to click on a link or call a phone number in an unsolicited text or email. If the message warns about fraud on your account and you don't want to simply ignore it, look up the phone number for that company's fraud department (it's on the back of your debit and credit cards) and call for guidance.

"These bad guys, this is what they do for a living," Murray said. They might send out tens of thousands of queries and get only one response, but that response could net them $10,000 from an unwitting victim. "Ten thousand dollars in one day for having one hit with one victim, that's a pretty good return on investment," she said. "That's what motivates them."

More to Read

Massive data breach that includes Social Security numbers may be even worse than suspected

2 hours ago

Editorial: A ransomware attack closed L.A. courts for two days. The public deserves a full accounting

Aug. 13, 2024

Column: Why hugely profitable corporations won't spend enough to keep hackers from stealing your private info

July 17, 2024

Jon Healey

Jon Healey writes and edits stories for the Los Angeles Times' Fast Break Desk, the team that dives into the biggest news of the moment. In his previous stints, he wrote and edited for the Utility Journalism team and The Times editorial board. He covered technology news for The Times from 2000 to mid-2005.