August 15, 2024 View online

THE CURRENT
TECH ALERTS

LATEST TECH ALERT

This impacts every American

National Public Data, a company that collects information from nonpublic sources without consent, according to a class-action **lawsuit** (paywall link)

sources without consent, according to a class-action lawsuit (paywall link), has been hit by a massive data breach. The company makes money by selling personal data to employers, private investigators and anyone conducting background checks.

Hacker group USDoD allegedly broke into National Public Data's unencrypted database before April 2024, making off with the records of a staggering 2.9 *billion* people. This breach not only affects every single American, but also individuals in the U.K. and Canada.

I know what you're thinking — the population of the U.S., U.K. and Canada is about 440 million. Keep in mind that some of the breached records include duplicates. For instance, if someone goes by two names or has multiple records for other reasons, those are all in the mix.

This breach is monumental, and it's safe to assume you're at risk. The hackers put the entire database — which includes Social Security numbers, full names and addresses — for sale on the Dark Web for $3.5 million.

Now, this is a shocker: No one bit, so they just handed it out for free. I know all these breaches and hacks start to feel like white noise, but you can't ignore this one.

Let's talk about your Social Security number

Think of it as the keys to the castle when it comes to your identity. You need to protect that number.

If yours is stolen and used for someone's gain, like opening up a loan or getting a job, start with the Federal Trade Commission's IdentityTheft.gov. Fill out the form there, and you'll get an entire plan for how to recover your identity and protect yourself going forward. **Here's an example.**

The IRS also has a place to report if you suspect someone is using your SSN: **Identity Theft Central**. Major red flags to watch for? You receive a tax form for a job you didn't do or you submit your taxes and there's already something on file.

You know things are bad when both the FTC and the IRS have dedicated portals to help you because someone is using your SSN and stealing from you.

Spot the signs

A fake tax form is one thing; most signs of identity theft are more subtle — at

A fake tax form is one thing; most signs of identity theft are more subtle — at least, in the beginning. Here's what to look for, along with steps to lock down your identity and protect your money:

- **Double-check all health care communications.** If you get an explanation of benefits (EOB) or bill for services you didn't receive, contact your health care provider and insurance company ASAP. It likely means someone is using your benefits for their *own* care.
- **Treat email requests with caution.** Be skeptical of anything that seems super urgent. It's OK to slow down for safety.
- **Freeze your credit.** This will keep scammers from opening a credit card or loan in your name. Like setting up a fraud alert, you'll need to **contact each of the three credit bureaus**. Watch out for bogus emails from the credit bureaus, too.
- **Be wary of "old friends" who appear out of nowhere.** It could be a hacker who happens to have a little (stolen) info. Take the time to confirm they are who they say they are.
- **Make a list of exposed data.** Keep this digitally or on a Post-it. Be suspicious of anyone who references it in an email or phone call. Say the company you financed your car through was hacked. Alarm bells should sound if you get a call out of the blue about a major issue with your loan.
- **Update your PIN and banking login credentials**, even if they weren't involved directly in a breach. Keep an eye on your bank and credit card statements for anything out of the ordinary. Set up banking alerts on your phone while you're at it.