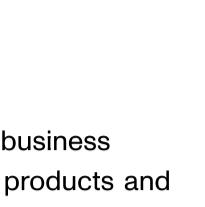
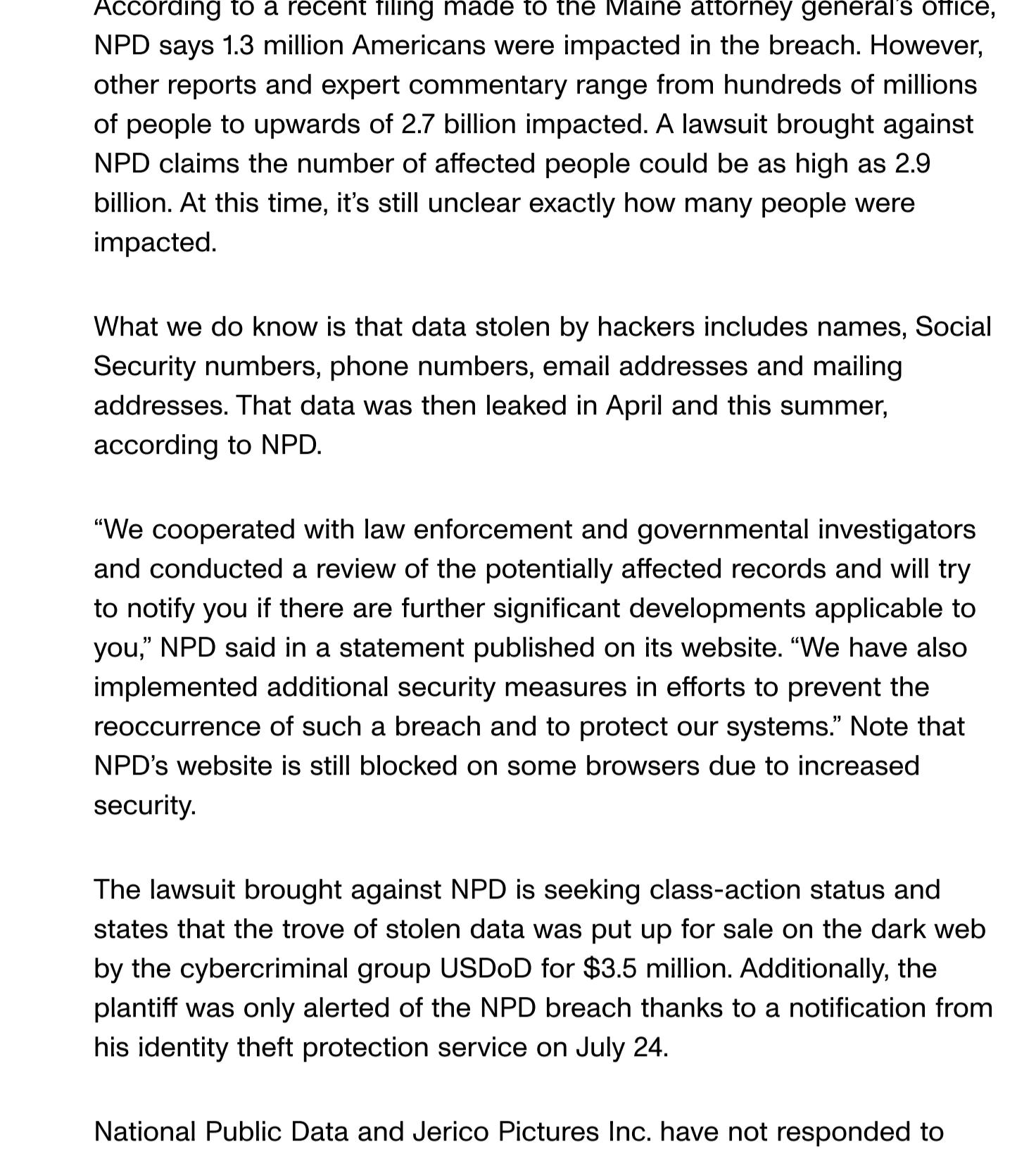


National Public Data Cyber Attack: Massive Data Breach Exposed Countless Social Security Numbers and Personal Info



You can't prevent data breaches, but there are steps you can take to keep your identity safe.

Advertiser Disclosure



Getty Images

More details about the cyberattack on National Public Data, a background check company owned by Jerico Pictures Inc., have come to light since the company's first public statement addressing the incident last week.

According to a recent filing made to the Maine attorney general's office, NPD says 1.3 million Americans were impacted in the breach. However, other reports and expert commentary range from hundreds of millions of people to upwards of 2.7 billion impacted. A lawsuit brought against NPD claims the number of affected people could be as high as 2.9 billion. At this time, it's still unclear exactly how many people were impacted.

What we do know is that data stolen by hackers includes names, Social Security numbers, phone numbers, email addresses and mailing addresses. That data was then leaked in April and this summer, according to NPD.

"We cooperated with law enforcement and governmental investigators and conducted a review of the potentially affected records and will try to notify you if there are further significant developments applicable to you," NPD said in a statement published on its website. "We have also implemented additional security measures in efforts to prevent the reoccurrence of such a breach and to protect our systems." Note that NPD's website is still blocked on some browsers due to increased security.

The lawsuit brought against NPD is seeking class-action status and states that the trove of stolen data was put up for sale on the dark web by the cybercriminal group USDoD for \$3.5 million. Additionally, the plaintiff was only alerted of the NPD breach thanks to a notification from his identity theft protection service on July 24.

National Public Data and Jerico Pictures Inc. have not responded to CNET's multiple requests for comment.

How to protect your identity after a data breach

Data breaches are popping up more frequently. More than 1,500 data breaches have occurred in the first half of 2024, impacting about 1 billion people, according to the Identity Theft Resource Center. This includes prominent breaches at AT&T and Ticketmaster this year.

If you're worried about this latest data breach or simply want to safeguard your personal data, there are steps you can take. Remember, just because your data was compromised in a data breach doesn't mean your identity will be stolen. However, bad actors will have more complete profiles of you if you're eventually targeted.

Luckily, there is plenty you can do to protect your identity.

Change your password

If you receive notice that your data was compromised in a breach, your first step should be to change your password for the affected account to avoid any unauthorized access. If you use the same password for other accounts, it's a good idea to update those too.

A good rule of thumb is to use a unique password for each online account. If you're finding this difficult to manage, try keeping your passwords safe with a password manager.

Watch out for phishing and smishing attempts

Be wary of targeted phishing and smishing attempts by cybercriminals looking to extract personal data from you. With so much information about us online and on social media, cybercriminals have become crafty about devising effective fraud schemes to dupe victims.

It's important to not click random links on your phone or email, which can lead to malicious software being downloaded onto your devices.

Also, don't provide your financial account information or Social Security number on a whim to anyone, as this can lead to unauthorized access into your bank accounts or even identity theft.

Sign up for identity theft protection

It might be worth signing up for identity theft protection if you're really concerned about your identity being stolen. Individual coverage ranges from \$7 to \$15 per month. Family plans are also available.

Services like Aura, CNET's top pick for identity theft protection, scan for your personal data on the dark web and monitor your credit and bank account activity. If your identity is stolen, the top identity theft protection companies will help restore your identity and provide insurance to cover stolen funds and necessary expenses.

OUR EXPERTS



Written by [Danni Santana](#)

Edited by [Courtney Johnston](#)

CNET staff -- not advertisers, partners or business interests -- determine how we review the products and services we cover. If you buy through our links, we may get paid.

[Reviews ethics statement →](#)

Why You Can Trust CNET Money

Our mission is to help you make informed financial decisions, and we hold ourselves to strict editorial guidelines. This post may contain links to products from our partners, which may earn us a commission. Here's a more detailed explanation of how we make money.

Advertisement

