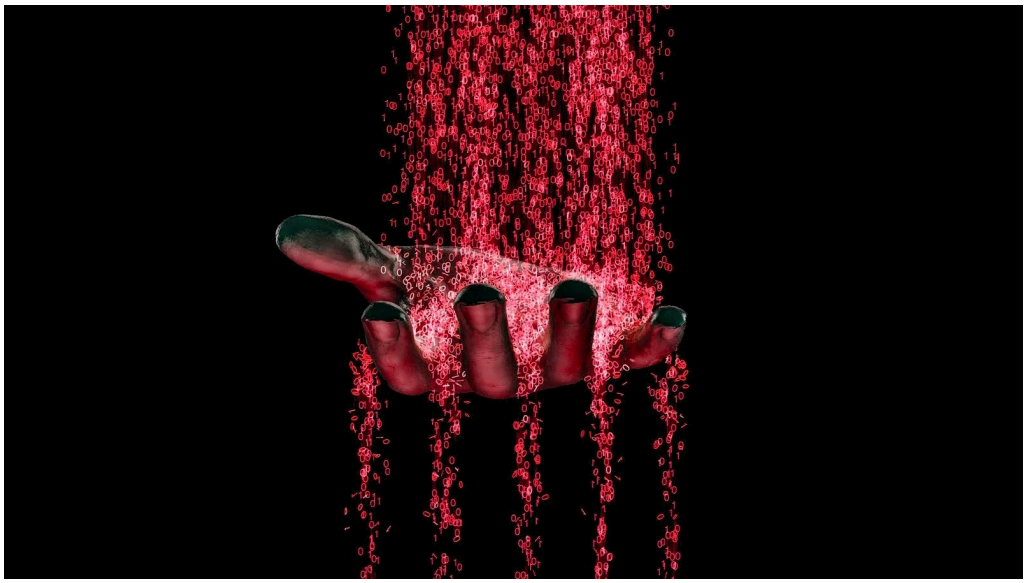
National Public Data confirms breach exposing Social Security numbers

By
Ionut Ilascu (https://www.bleepingcomputer.com/author/ionut-ilascu/)

August 16, 2024 01:18 PM 1



Background check service National Public Data confirms that hackers breached its systems after threat actors leaked a stolen database with millions of social security numbers and other sensitive personal information.

The company states that the breached data may include names, email addresses, phone numbers, social security numbers (SSNs), and postal addresses.

Breach linked to late 2023 hack attempt

In the statement disclosing the security incident, National Public Data says (https://nationalpublicdata.com/Breach.html) that “the information that was suspected of being breached contained name, email address, phone number, social security number, and mailing address(es).”

According to Troy Hunt, the creator and maintainer of the Have I Been Pwned (HIBP (https://haveibeenpwned.com/)) search service for compromised personal data, there were 134 million unique email addresses (https://www.troyhunt.com/inside-the-3-billion-people-national-public-data-breach/) in one version of the NPD leaked database he analyzed.

Not all the information may be accurate, though. Tests from BleepingComputer showed that some people were associated with someone else's name.

Hunt's analysis of the dataset he received seems to confirm this, as he found one of his email addresses associated with two unique dates of birth, none of them his.

Furthermore, BleepingComputer found that some of the details in the database may also be outdated, as it does not include the current address of any of the people we checked.

Inaccuracies aside, the NPD incident has led to at least one class action lawsuit against Jerico Pictures (https://www.documentcloud.org/documents/25038487-hoffman-npd-class-action-lawsuit), the entity that operates the National Public Data service.

NPD is believed to source their details from public files such as government records (federal, state, and local), which include all legal papers related to an individual.

People impacted by the NPD breach should monitor financial accounts for signs of potentially fraudulent activity and report it to credit bureaus.

Because contact information is present in the leak, there is also the possibility of phishing attempts to trick you into providing more sensitive details that could be used for fraudulent activities.