National Public Data Security Breach: What You Need to Know & Best Preventative Practices to Follow

PLEASE NOTE: This data breach is not associated with Citizens Savings Bank in any way.

Citizens Savings Bank wants to make you aware of the recent data breach at National Public Data in April 2024, a background checking company. Per their website, "[NPD obtains] information from various public record databases, court records, state and national databases, and other repositories nationwide." The breach included the possibility of stolen data including Social Security numbers and other Personally Identifiable Information (PII). While the number of impacted individuals continues to fluctuate, the total number of impacted individuals is believed to be lower than was initially reported by many media outlets since many of the records stolen belonged to the deceased. Please review the article below for more details.

Data Breach Exposes 3 Billion Personal Information Records | McAfee Blog

BACKGROUND:

A hacker known as "USDoD" allegedly hacked a company called National Public Data and stole personal records. The compromise is believed to have begun in or around April 2024, after which the records were posted for sale and later released by other criminal groups onto the dark web. Currently available information suggests this was a compromise of personal information, not credit and debit card information. At this time, we do not believe card data was tied to this event.

Additionally, Citizens Savings Bank recommends the following industry best practices for actions to take, including but not limited to the following:

- Cardholders should update their antivirus protection and perform security scans on all devices. If malware is found most antivirus programs should be able to remove it, but they may need to seek reputable professional assistance in some cases.
- Cardholders should update passwords for bank accounts, email account, social media accounts, and other services used, ensuring their updated passwords are strong and unique for each account. Passwords should include uppercase and lowercase letters, numbers, and special characters whenever possible and should never include personal information that a hacker could guess or obtain from stolen data.
- The use of multifactor authentication is recommended on any accounts or services that offer it to ensure proper identity verification.
- Cardholders are encouraged to check their credit report and report any unauthorized use of credit cards. If they notice any suspicious activity, cardholders can ask credit bureaus to freeze their credit.

Citizens Savings Bank recommends using extra caution with email and social media accounts and beware of phishing, which is an attempt to get your personal information or access to accounts by misrepresenting the identity of person or entity sending a message.

Citizens SAVINGS BANK