Advance Auto Parts data breach impacts 2.3 million people

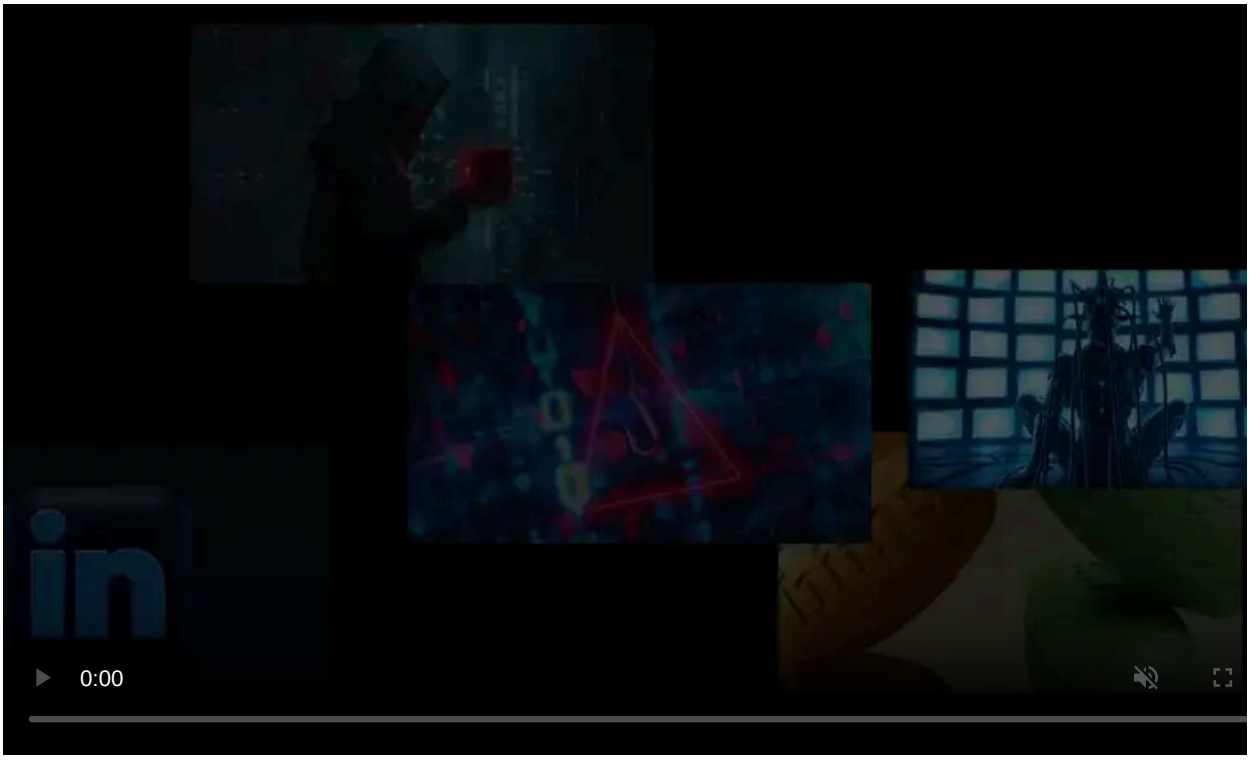
By Bill Toulas

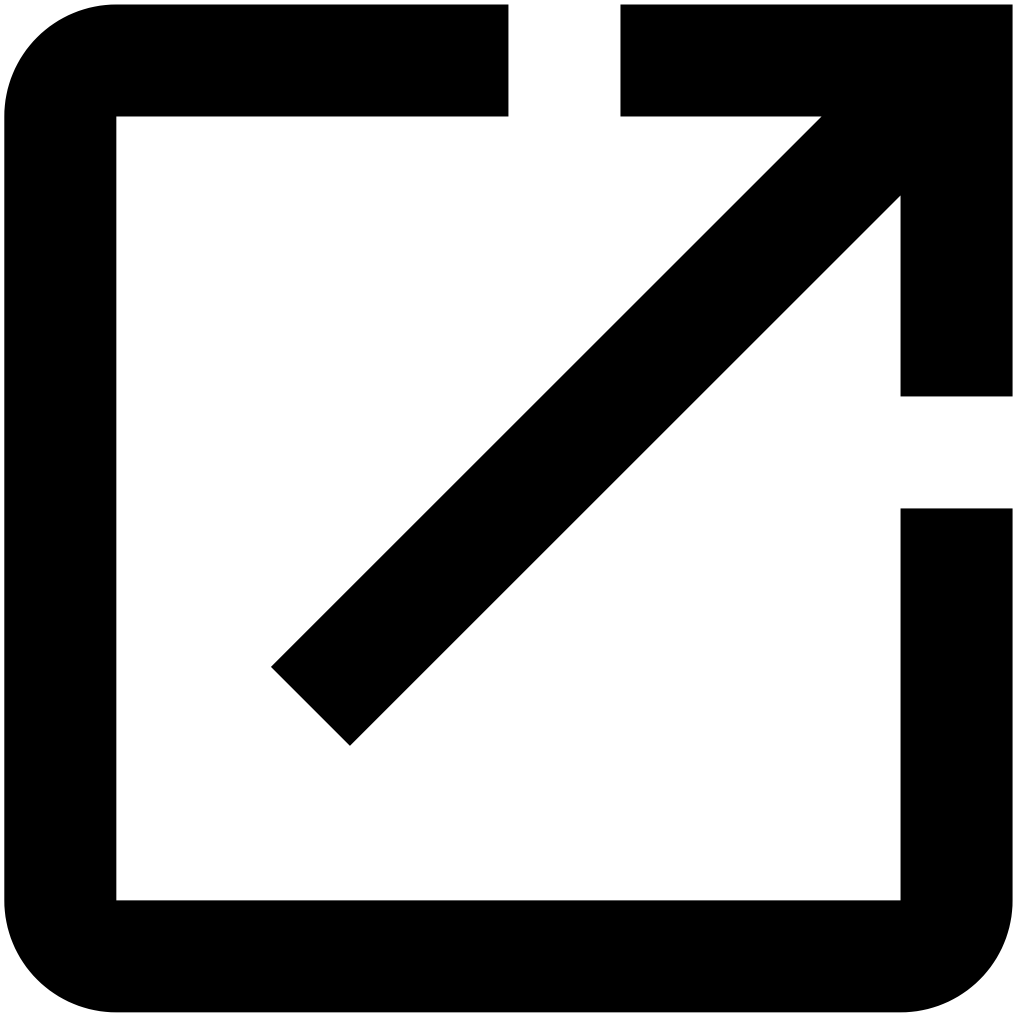
Published: 2024-07-11 · Archived: 2026-04-05 15:46:58 UTC

Advance Auto Parts is sending data breach notifications to over 2.3 million people whose personal data was stolen in recent Snowflake data theft attacks.

Advance operates 4,777 stores and 320 Worldpac branches, serving 1,152 independently owned Carquest stores in the United States, Canada, Puerto Rico, the U.S. Virgin Islands, Mexico, and various Caribbean islands.

On June 5, 2024, a threat actor known as 'Sp1d3r' began selling a massive 3TB database allegedly containing 380 million Advance customer records, orders, transaction details, and other sensitive information.


0:00



On June 19, the company confirmed the breach via a Form 8-K filing but said it only impacts current and former employees and job applicants.

The incident was part of a broader campaign targeting Snowflake accounts using stolen credentials, which impacted Pure Storage, Los Angeles Unified, Neiman Marcus, Ticketmaster, and Banco Santander.

Employees impacted

Advance has completed its internal investigation into the incident and has determined that the data breach impacted 2,316,591 million people.

According to the data breach notification samples shared with the authorities, the threat actors maintained unauthorized access to Advance's Snowflake environment for over a month, starting mid-April 2024.

"Our investigation determined that an unauthorized third party accessed or copied certain information maintained by Advance Auto Parts from April 14, 2024, to May 24, 2024," reads the notice.

"We conducted a detailed review and analysis of the affected information to determine the types of information contained therein and to whom the information relates."

The data stolen by the attackers includes full names, Social Security numbers (SSNs), driver's licenses, and government ID numbers.

The company says it collects this information as part of its job application process, so the 2.3 million figure is related to job applicants and former/current employees whose data was stored in the compromised cloud database.

Those impacted are given 12 months of complimentary identity theft protection and credit monitoring services through Experian, and they have until October 1, 2024, to enroll.

Potentially impacted individuals are advised to be vigilant for unsolicited communications, monitor their accounts closely, activate fraud alerts, and consider placing a credit freeze.

The 2.3 million figure reported by Advance is a far cry from the threat actor's allegations about 380M records, and the data types confirmed to have been exposed aren't nearly as extensive as what 'Sp1d3r' offered for sale.

However, samples of the stolen data seen by BleepingComputer appear to have contained customer information, so it's possible they will be notified in the future.

BleepingComputer contacted Advance Auto Parts to clarify whether customer information was exposed, but a comment wasn't immediately available.
