AT&T Data Breach Exposes Millions to Identity Theft and Privacy Risks

March 31, 2024 - On Saturday, telecommunications giant AT&T disclosed that data belonging to approximately 73 million current and former account holders has been leaked onto the dark web. The breach, which affects around 7.6 million current customers and a staggering 65.4 million former customers, presents grave implications for both privacy invasions and identity theft.

The compromised data, believed to originate from 2019 or earlier, includes a trove of sensitive information such as passcodes, full names, email addresses, home addresses, phone numbers, dates of birth, and Social Security numbers. That is absolutely everything needed to commit identity theft. It is a comprehensive data set.

AT&T has responded to the breach by resetting passcodes for the affected current account holders and is offering complimentary identity theft and credit monitoring services to individuals with compromised sensitive personal information.

According to a report in the Epoch Times, a security researcher named Troy Hunt obtained the full data set, corroborated the severity of the breach by confirming its authenticity and the substantial impact it poses. According to his observations, the data set included more than 44 million social security numbers.

The incident raises serious concerns about the efficacy of AT&T's cybersecurity measures. One of the most disturbing aspects of this breach is the fact that AT&T is publicly stating that there is no evidence their servers were involved in the breach. But they apparently don't know if one of their vendors has been compromised or if the breach happened in some other way.

At this point, it isn't clear if the breach only includes AT&T's telecommunications customers or if other areas of the business, such as DirecTV, were also included in the breach. Therefore, consumers who have been customers of any AT&T company should assume that their data was included in the breach until AT&T announces otherwise.

Anyone who believes that they may have been included in the breach should consider freezing their credit files. This will prevent any bad actors from opening new lines of credit in their name. Additionally, consumers should check all of their regular bills thoroughly to make sure there are no fraudulent charges on them. The data set that was breached also included more than 40 million email addresses. Because of this, AT&T's current and former customers should be very careful about clicking on email links or downloading files as these may lead to the installation of malware on their computers.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS