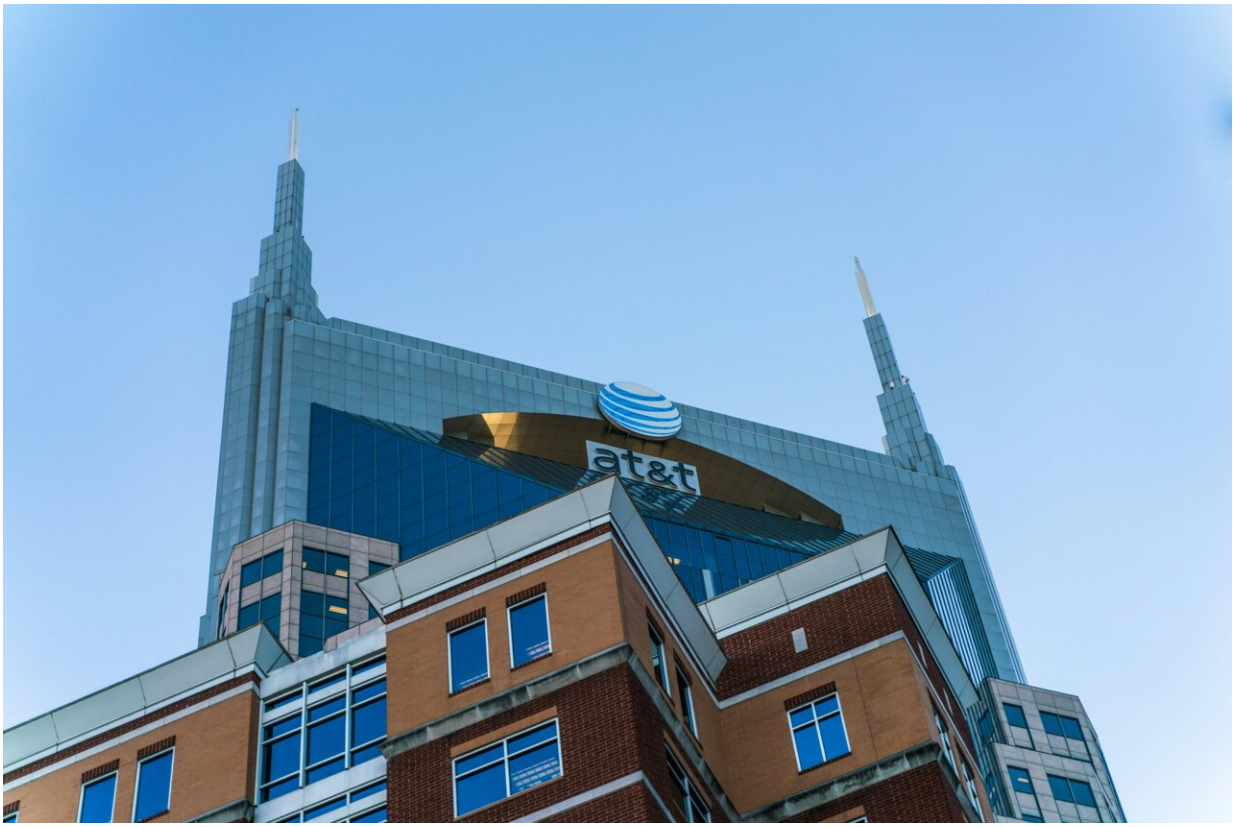
Five things to know about the AT&T data breach

July 15 2024, by Emily Bloch, The Philadelphia Inquirer



Credit: Unsplash/CC0 Public Domain

AT&T says calls and text message records for tens of millions of the phone service provider's customers were exposed in a massive data breach two years ago.

The company announced Friday that nearly all of its mobile phone customers' information was exposed over the course of months in 2022. The data stolen includes "records of calls and texts of nearly all of AT&T's cellular customers," AT&T said in a statement.

It marks one of the largest private communications data breaches in recent history, Bloomberg reports.

Here's what we know.

How did AT&T get hacked?

AT&T said it learned about an "illegal download" of data from a third-party cloud platform called Snowflake (more on that later) in April. The news came about a month after the company was dealing with a separate data leak where customers' personal information was posted on the dark web. AT&T told CNN the data leak and freshly announced breach are unrelated.

The company said it hired experts to investigate the cloud data's compromise after a "threat actor" said they "unlawfully accessed and copied" AT&T's call logs on April 19. AT&T said Friday that experts determined that the hackers accessed files from April 14 to 25.

According to AT&T, the U.S. Department of Justice directed the company to delay its disclosure to the public. In a statement provided to The Inquirer, the FBI confirmed a delay in public disclosure citing an SEC rule regarding public safety. The Justice Department and FBI confirmed both agencies were working with AT&T in an ongoing investigation.

What AT&T data was stolen?

Compromised data includes the following, according to AT&T:

- Telephone numbers of "nearly all" AT&T cellular customers from May 1 through Oct. 31, 2022
- Telephone numbers of customers of wireless providers that use AT&T's network from May 1 through Oct. 31, 2022
- Phone logs of the aforementioned customers, which include records of every number customers texted — including people on other wireless networks — along with the number of times they interacted
- Phone logs of the aforementioned customers with records of every number they called — including people on other wireless networks — and how long the calls lasted

The records of a "very small" number of customers on Jan. 2, 2023 were also exposed, AT&T said. Landline customers with AT&T who interacted with the cell numbers of those impacted were also compromised.

AT&T also said that for an undisclosed subset of its exposed records, at least one cell site identification number linked to texts or calls were exposed, which could reveal some customers' broad location details. The company did not provide additional details.

AT&T had about 110 million wireless subscribers at the end of 2022, according to the company.

What wasn't stolen?

AT&T says call and text message content wasn't exposed. It also says international calls weren't included in the stolen data except for calls to Canada. The specific time texts or calls occurred was not exposed.

Customer's names weren't exposed in the hack, AT&T said. Still, the company acknowledged that publicly available tools can sometimes link phone numbers to people's names.

The breach does not contain customers' personal information, like birthdays or social security numbers.

Was I affected by AT&T's data breach?

AT&T said "nearly all" of its customers at the time were affected. The breach included customers who used the service provider between May 1 through Oct. 31, 2022. Landline AT&T customers and people who used other service providers but interacted by phone or text with AT&T cell service customers during this same period may have also been affected.

Additionally, that "very small" number of customers on Jan. 2, 2023, may have also been exposed.

The company said it would notify current and former customers whose information was involved and would provide resources to help protect their information.

What is Snowflake?

AT&T said its customer data was illegally downloaded from its workspace on a third-party cloud platform. According to CNN, that platform is Snowflake.

Snowflake is a data warehousing and data engineering platform that promotes itself as a place for companies that deal with data to organize and manage information.

Other Snowflake customers include JetBlue, Mastercard, Canva, and Orangetheory, according to the platform's website.

Snowflake's chief information security officer told CNN that the company hasn't found evidence that the hack was "caused by a vulnerability, misconfiguration or breach of Snowflake's platform."