Massive AT&T data breach exposes call logs of 109 million customers

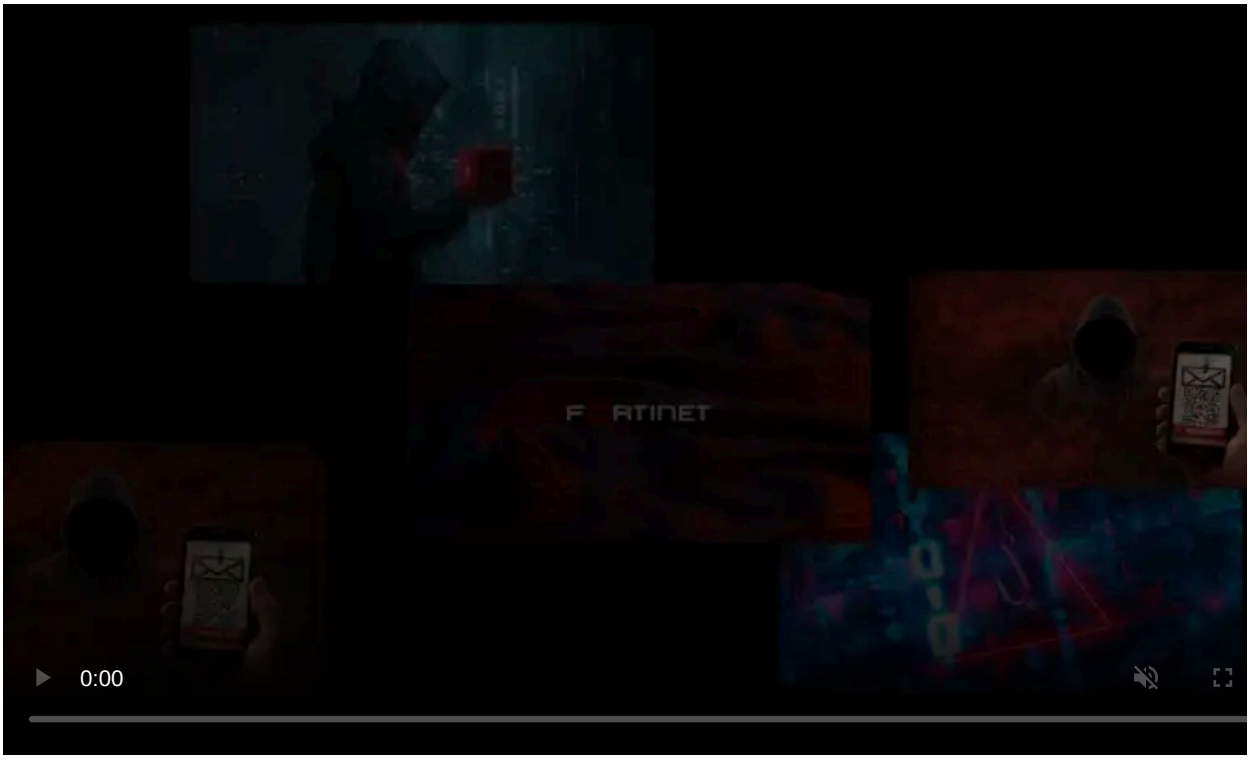
By Bill Toulas

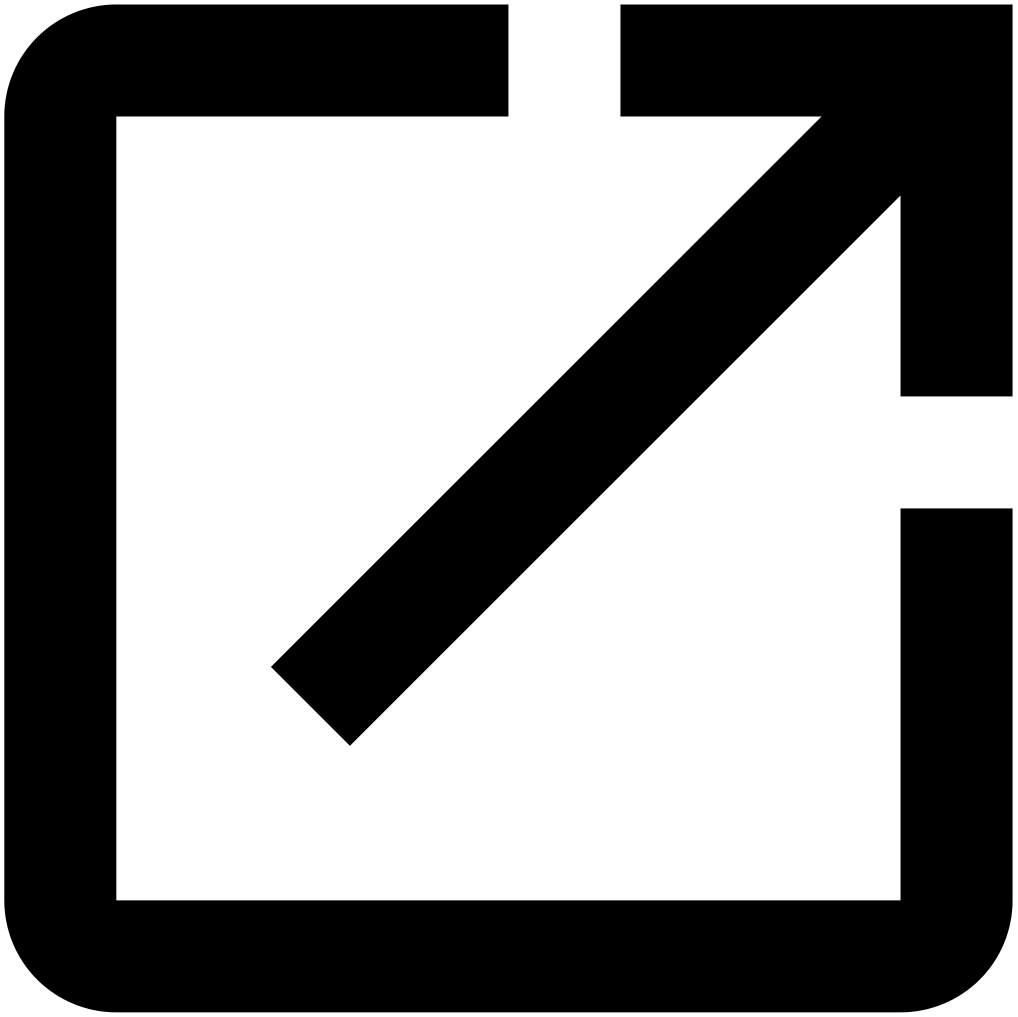
Published: 2024-07-12 · Archived: 2026-04-05 21:10:26 UTC

AT&T is warning of a massive data breach where threat actors stole the call logs for approximately 109 million customers, or nearly all of its mobile customers, from an online database on the company's Snowflake account.

The company confirmed to BleepingComputer that the data was stolen from the Snowflake account between April 14 and April 25, 2024.

In a Friday morning Form 8-K filling with the SEC, AT&T says that the stolen data contains the call and text records of nearly all AT&T mobile clients and customers of mobile virtual network operators (MVNOs) made from May 1 to October 31, 2022 and on January 2, 2023.


F RTINET
0:00



The stolen data includes:

- Telephone numbers of AT&T wireline customers and customers of other carriers.
- Telephone numbers with which AT&T or MVNO wireless numbers interacted.
- Count of interactions (e.g., the number of calls or texts).
- Aggregate call duration for a day or month.
- For a subset of records, one or more cell site identification numbers.

The exposed records did not contain the content of the calls or texts, customer names, or any other personal information such as Social Security numbers or dates of birth.

Although the accessed logs do not contain sensitive information that directly exposes customer identities, the communications metadata can be used to correlate them with publicly available information and easily derive identities in many cases.

The company says that after learning of the breach they worked with cybersecurity experts and notified law enforcement. The US Department of Justice gave AT&T permision twice, on May 9, 2024 and June 5, 2024, to delay public notification due to the potential risks to national security and public safety.

"Shortly after identifying a potential breach to customer data and before making its materiality decision, AT&T contacted the FBI to report the incident. In assessing the nature of the breach, all parties discussed a potential delay to public reporting under Item 1.05(c) of the SEC Rule, due to potential risks to national security and/or public safety," the FBI told BleepingComputer.

"AT&T, FBI, and DOJ worked collaboratively through the first and second delay process, all while sharing key threat intelligence to bolster FBI investigative equities and to assist AT&T's incident response work."

"The FBI prioritizes assistance to victims of cyber-attacks, encourages organizations to establish a relationship with their local FBI field office in advance of a cyber incident, and to contact the FBI early in the event of breach."

AT&T is working with law enforcement to arrest those involved and states that they understand at least one person has already been apprehended.

AT&T said it has implemented additional cybersecurity measures to block unauthorized access attempts in the future, and it promised to notify current and former customers impacted by this incident soon.

Meanwhile, AT&T customers can follow the links provided on this FAQ page to check if their phone number's data was exposed and to download the data associated with their number that was stolen.

As of today, AT&T says it has no evidence the accessed data has been made publicly available and says the incident is not related to the 2021 data breach AT&T confirmed earlier this year impacted 51 million customers.

The Snowflake data theft attacks

AT&T has confirmed to BleepingComputer that the data was stolen from its Snowflake account as part of a wave of recent data theft attacks using compromised credentials.

Snowflake is a cloud-based database provider that allows customers to perform data warehousing and analytics on large volumes of data.

Last month, Mandiant revealed that a financially motivated threat actor tracked as 'UNC5537' was behind multiple attacks against Snowflake customers, using account credentials stolen via infostealer malware.

Snowflake has since introduced a mandatory multi-factor authentication (MFA) enforcement option for workspace administrators to protect accounts against easy take-overs leading to data breaches impacting millions of people.

The list of high-profile victims to which AT&T is being added now includes Advance Auto Parts, Pure Storage, Los Angeles Unified, Neiman Marcus, Ticketmaster, and Banco Santander.

Source: https://www.bleepingcomputer.com/news/security/massive-atandt-data-breach-exposes-call-logs-of-109-million-customers/