



ICE'S DATA BREACH CASE STUDIES

AT&T

WHAT HAPPENED?

Nearly all AT&T cell customers' call and text records were exposed in a massive breach.

AT&T disclosed a significant data breach, revealing that the call and text records from mid-to-late 2022 of tens of millions of its customers, as well as non-AT&T customers, were compromised. The exposed data includes the phone numbers of "nearly all" cellular customers and those of wireless providers using AT&T's network from May 1, 2022, to October 31, 2022. The stolen information comprises details of all calls and texts made by AT&T customers, as well as interactions with customers of other networks, along with call durations. Notably, the breached data does not contain the contents or timing of the communications. Furthermore, records of a few customers from January 2, 2023, were also affected. The FCC stated on the X social media platform that they are actively investigating the breach in collaboration with law enforcement agencies. AT&T attributed the breach to an "illegal download" from a third-party cloud platform, which came to their attention in April, coinciding with another major data leak incident. While AT&T claims the exposed data is not publicly accessible, CNN could not independently verify this assertion.

AT&T spokesperson Alex Byers informed CNN that this recent incident is completely unrelated to a previous one revealed in March. During the prior disclosure, AT&T reported that sensitive information, including Social Security numbers, of 73 million past and present customers had been exposed on the dark web.

"We sincerely regret this incident occurred and remain committed to protecting the information in our care," the company said in a statement about the latest breach.

AT&T reported around 110 million wireless subscribers by the end of 2022. Notably, the stolen data excluded international calls, except for those to Canada. The breach impacted AT&T landline customers connected to these cellular numbers.



888-423-4801

www.iceconsulting.com

info@iceconsulting.com

While the breach did not expose the contents of calls or texts, sensitive personal details like Social Security numbers, birthdates, or customer names remained secure. However, AT&T acknowledged that publicly accessible tools can sometimes link names to specific phone numbers.

Moreover, AT&T revealed that a subset of its records, albeit undisclosed, had one or more cell site identification numbers linked to the calls and texts compromised. This data could potentially reveal the general geographical whereabouts of one or more individuals involved in the communications.

AT&T reported that at least one individual linked to the cybercrime incident is in custody, as stated in a submission to the Securities and Exchange Commission. The FBI chose not to respond to inquiries regarding this claim.

AT&T pledged to inform both current and former customers affected by the breach, offering them resources to safeguard their data. Furthermore, details like call times and message timestamps remained uncompromised. Nonetheless, AT&T's representative, Byers, informed CNN that specific data, including call and text volumes, as well as total call durations for given periods, were exposed.

This indicates that while the leaked data does not pinpoint the exact timing of calls between two numbers, it could disclose the frequency of communication and the durations of these interactions on particular dates.

AT&T said it learned on April 19 that a "threat actor claimed to have unlawfully accessed and copied AT&T call logs." The company said it "immediately" hired experts and a subsequent investigation determined hackers had exfiltrated files between April 14 and April 25.

WHY THE JUSTICE DEPARTMENT DELAYED PUBLIC DISCLOSURE

The company stated that the US Department of Justice found it necessary to delay public disclosure in May and June. Following the discovery of the hack, AT&T contacted the FBI promptly. However, the FBI opted to review the data to assess any potential risks to national security or public safety.

"In assessing the nature of the breach, all parties discussed a potential delay to public reporting... due to potential risks to national security and/or public safety," the FBI said in a statement. "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."



This seems to mark the initial cyber incident where the Justice Department has requested a company to postpone submitting a disclosure to the SEC due to possible national security or public safety issues.

"This is very concerning. This information is very valuable to cyber criminals and to nation-states," Sanaz Yashar, co-founder and CEO of cybersecurity firm Zafran, told CNN.

Yashar, a former Israeli cyber operative, highlighted that threat actors have the ability to cross-reference cell ID data with other readily accessible information to accurately determine an individual's workplace, even at high-security sites such as the White House and Pentagon.

"You don't need the timestamp. If someone is there everyday, you can understand they work there and their routine. This is very secret information and a way that spies do stuff." Justin Sherman, founder of Global Cyber Strategies, a consultancy, also put the potential threat in stark terms.

"Metadata about who's communicating with who, at massive scale, enables someone to map connections between people — think journalists and sources, intelligence officers and their contacts, married people and those with whom they're having an affair," Sherman told CNN.

Jason Hogg, a former FBI special agent who is now executive-in-residence at Great Hill Partners, said the cell site data is "quite significant because it could allow bad actors to determine certain consumers' geolocation, which could be used to make the social engineering attacks more believable."

AT&T shares fell 1% on Friday following the news.

In the recent incident, AT&T informed CNN that it became aware in April of unauthorized downloading of customer data from its workspace on Snowflake, a third-party cloud platform.

AT&T joins a growing list of major corporations falling victim to data breaches through their



Snowflake platform. Ticketmaster and Santander Bank have similarly reported significant data breaches tied to Snowflake. Mandiant, a cybersecurity firm under Google's umbrella, has alerted approximately 165 organizations that they could potentially be impacted by this hacking wave.

Brad Jones, chief information security officer at Snowflake, told CNN in a separate statement that the company has not found evidence this activity was "caused by a vulnerability, misconfiguration or breach of Snowflake's platform." Jones said this has been verified by investigations by third-party cybersecurity experts at Mandiant and CrowdStrike.

AT&T said it launched an investigation, hired cybersecurity experts and took steps to close the "illegal access point."

Protecting your business from becoming the next news headline!

ICE Consulting has served as a Managed Cybersecurity Provider for more than 26 years. Our expertise lies in enhancing businesses' security stance and delivering a range of cybersecurity services including:




1. Security Operation as a Service (24x7 real time cyber threat monitoring and response services)
2. Incident Response Planning
3. Security & Network Vulnerability Scans
4. Penetration testing
5. Cybersecurity Training

As data breaches reach record levels and show no signs of slowing down, it's crucial for every business to regularly evaluate its security stance for weaknesses. We offer this service at no charge to businesses. Reach out today to discover more about this process.




ICE Consulting, Inc
Managed Cybersecurity Provider



 888-423-4801
 info@iceconsulting.com
 www.iceconsulting.com



 888-423-4801

 www.iceconsulting.com

 info@iceconsulting.com