Shumaker

NOVEMBER 13, 2025 | PUBLICATION

"Post Mortem Review of AT&T Breaches"

Data breaches occur when an unauthorized individual or entity gains access to confidential or protected information.[1] This information may include personal data such as Social Security numbers or medical records, financial information, intellectual property, or login credentials.[2] These data breaches may be the result of cyberattacks, insider threats, or even simple human errors.[3] Common causes may include phishing attacks, malware or ransomware, weak or stolen passwords, misconfigured cloud storage, insider negligence, or simply malicious intent.[4]

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Andrew R. DeWeese

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

As cybersecurity threats continue to evolve, several recent high-profile data breaches and security incidents have affected major organizations, including AT&T, a leading telecommunications company that provides services such as mobile, internet, and business networks.[5] AT&T announced two major data breaches in 2024, and estimates suggest the breaches impacted over seven million people with AT&T accounts in 2024 and over 65 million account holders from 2019-2024. This ultimately led to multiple class-action lawsuits and a $177 million settlement.

The first set of lawsuits stemmed from a 2019 data breach that wasn't announced until March 30, 2024. According to legal filings, the breach occurred when hackers stole addresses, birthdates, Social Security numbers, and other data belonging to 7.6 million current AT&T customers and 65.4 million former account holders.[6] In a 2025 class-action lawsuit, plaintiffs alleged the perpetrators began selling the information on the dark web in 2021.[7] One plaintiff claimed a CareCredit account opened in her name racked up approximately $12,000.[8] Another plaintiff reported being so overwhelmed with spam calls and texts that she had to file a police report and change her number.[9] AT&T initially denied the breach before finally acknowledging the incident in March 2024.[10]

The second set of lawsuits followed a cyber event on July 12, 2024, where AT&T data stored in a third-party cloud platform hosted by Snowflake, Inc. was compromised. According to records, hackers accessed phone numbers, call durations, cell site identification numbers, and other data from "nearly all of AT&T's wireless customers" during a six-month period in 2022.[11] The stolen data mostly included mobile and landline numbers, call and text logs from AT&T's network, aggregate call duration, and some cell site identification numbers.[12] This data may have been enough to figure out the identities of AT&T customers.[13]

Separate lawsuits were filed over both data breaches before being consolidated into a single class-action lawsuit. AT&T denied any wrongdoing in either case, stating that it opted to settle "to avoid the expense and uncertainty of protracted litigation."[14]

The actions were initially litigated in tandem (respectively, in the North Distrct of Texas and the District of Montana) before the parties ultimately settled the lawsuits together in March 2025. The parties reached a class-action settlement "without any admission of liability or wrongdoing"; however, AT&T still faces settlement payments amounting to approximately $177 million in addition to legal fees, costs, and other remediation expenses.[15]

According to AT&T's full-year consolidated earnings results for 2024, the company saw $122.3 billion in revenues and free cash flow of $17.6 billion.[16] AT&T also reported 1.7 million postpaid phone additions and 1 million fiber net additions, indicating an expanding user base—which also suggests more account owners and data elements in AT&T's possession.[17] Although $177 million is no small sum, one could consider it a manageable blemish for a company with revenue over $120 billion. Time will tell if AT&T's additional response and remediation efforts will render this settlement a small price to pay for a big lesson.

The consequences of a data breach can be severe and may result in financial loss, reputational damage, operational disruption, and legal and regulatory penalties.[18] In responding to a potential breach, it is essential for organizations to implement a swift and strategic response, including steps such as identifying and containing the breach, assessing the scope and impact of the breach, notifying affected parties and regulatory bodies immediately, and reviewing and strengthening security policies.

Organizations can proactively reduce risk by heightening security measures such as implementing stronger access controls and utilizing encryption. Data breaches and security incidents are not just IT problems; they are business risks. Organizations must treat cybersecurity as a strategic and compliance priority, investing in technologies, processes, and individuals that safeguard their digital assets. The cost of prevention is always lower than the cost of recovery.

If you have questions or would like more information, please contact Andrew DeWeese, Enisha Smith, or a member of Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line.

---

[1] https://hrpp.research.virginia.edu/teams/irb-hsr/researcher-guide-irb-hsr/data-breach

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] https://about.att.com/pages/what-we-do#:~:text=AT&T%20is%20a%20company%20that%20creates%20conne

ctions,in%20the%20wake%20of%20unpredictable%2C%20catastrophic%20events

[6] https://www.cnbc.com/select/claim-your-share-of-the-177-million-att-data-breach-settlement/#:~:text=Impacted%20customers%20could%20receive%20up,65.4%20million%20former%20account%20holders.

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] https://www.yahoo.com/news/articles/t-settles-177-million-data-224553616.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAL2Ymegm5z5wqnZB3sswlGXWvLc_Pb-Jmxp6Se5ARYBovjNlkQBCCu-UnGNSfFG0pwHLiQqx16HPb3GdltQ6lfOU7qhxZNqGCBremi7_upMTNILUDXj4XSTFjYLRn4_0LXxdwqfpxBCP80jvv4BJsc3CflzFuT1XdIrv_A4JbLs1

[13] *Id.*

[14] https://www.cnbc.com/select/claim-your-share-of-the-177-million-att-data-breach-settlement/#:~:text=Impacted%20customers%20could%20receive%20up,65.4%20million%20former%20account%20holders.

[15] https://www.telecomdatasettlement.com/

[16] https://about.att.com/story/2025/4q-earnings-2024.html

[17] *Id.*

[18] https://www.securityweek.com/category/data-breaches/

© 2026 Shumaker, Loop & Kendrick, LLP. All Rights Reserved. Privacy Policy/Disclaimer