United States Senate
WASHINGTON, DC 20510

July 16, 2024

John Stankey
Chief Executive Officer
AT&T
208 S Akard St
Dallas, T.X. 75202

Dear Mr. Stankey,

We write demanding information regarding the breach of AT&T's private customer data and seek answers about how AT&T failed to protect such profoundly sensitive information from cybercriminals.

On July 12, 2024, AT&T announced that six months of customer data, including phone call and text message records, were illicitly accessed from a third-party cloud platform, the vendor Snowflake.[1] While the records do not directly include names and addresses, as AT&T's Securities and Exchange Commission filing notes, the stolen data includes location information and it is easy to find the name associated with a phone number. Taken together, the stolen information can easily provide cybercriminals, spies, and stalkers a logbook of the communications and activities of AT&T customers over several months, including where those customers live and traveled — a stunning and dangerous breach of its customers' privacy and intrusion into their personal lives.

The theft of AT&T subscriber information appears to be connected with an ongoing series of breaches of clients of Snowflake, a cloud service designed to help companies analyze business data. In addition to AT&T, other companies including Ticketmaster, Advance Auto Parts, and Santander Bank, have announced breaches of customer or employee information hosted on their Snowflake services. While AT&T is the latest Snowflake customer to disclose a breach, according to the cybersecurity firm Mandiant, 160 other organizations also appear to have been targeted in the hacking campaign. [2]

[1] "Unlawful access of customer data." AT&T. https://www.att.com/support/article/my-account/000102979
[2] "UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion." Mandiant. https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

Disturbingly, the AT&T breach appears to have been easily preventable. While Snowflake, AT&T, and other clients have avoided taking direct responsibility, according to Mandiant, it appears that the cybercrime group behind the breaches obtained companies' passwords from malware infections, including malware bundled with pirated software. Compounding this basic cybersecurity failure, the hacked accounts had often kept the same passwords for several years, failed to implement firewall access, and failed to turn on multi-factor authentication — additional basic cybersecurity failures that seemingly reflect gross negligence, particularly in light of the sensitivity of the data stolen in many of the breaches.

AT&T customers, including businesses and government entities, should be deeply concerned about this theft private information about their communications. While AT&T stated that it "do[es] not believe the data is publicly available," the group behind the breach, ShinyHunters, has already leaked records of Ticketmaster customers, demanded ransoms, and offered for public sale large sets of data stolen from Snowflake customers. These criminal operations continue, as recently as this month advertising the sale of ticket information of 166,000 Taylor Swift fans. There is no reason to believe that AT&T's sensitive data will not also be auctioned and fall into the hands of criminals and foreign intelligence agencies.

Given this alarming and seemingly preventable theft of highly-sensitive customer information, we ask for your responses to the following questions by July 29, 2024:

1. How did the hackers behind the AT&T breach initially gain access to its Snowflake services and download customer information? Did the breach include information stolen from a contractor, and if so, who is the contractor?

2. Please provide a detailed timeline of all events related to the breach, including the date and background on the discovery, response, and remediation of compromised systems or disabled services.

3. The Snowflake breach is the second report of AT&T customer records being obtained by cybercriminals this year. Please provide information on any investigation into the reported leak of 73 million records that was announced this March.[3]

4. According to AT&T's disclosure, the data stolen in the attack includes phone call and text message records of nearly all of its cellular customers, including location information. Please provide a full accounting of the types of data stolen from AT&T and how that data was linked together in a manner that would impact the privacy of customers.

5. According to AT&T's disclosure, the breach includes customers of mobile virtual network operators (MVNOs), other phone companies that rely on AT&T's network. As a result, the impact of this breach goes beyond direct AT&T customers. Which MVNOs were affected by the breach and have those MVNOs been notified of the breach? Is

[3] "AT&T admits massive 70M+ mid-March customer data dump is real though old." The Register. https://www.theregister.com/2024/04/01/att_admits_massive_70m_midmarch/

AT&T working with the MVNOs to ensure that appropriate customer notifications are conducted?

6. How does AT&T plan to individual notify customers regarding their compromised data and what information, support, and compensation will AT&T provide to customers to protect them from this intrusive breach of their privacy? Will AT&T be extending the same information, support, and compensation to customers of affected MVNOs?

7. Why had AT&T retained months of detailed records of customer communication for an extended amount of time and why had AT&T uploaded that sensitive information onto a third party analytics platform? What is AT&T policy, including timelines, concerning retaining and using such information?

8. Why did AT&T delay public notice of the breach, and when did it notify law enforcement about the breach of customer records, including records that may have national security implications?

Thank you for your attention to this important matter.

Sincerely,

Richard Blumenthal
Chair
Subcommittee on Privacy, Technology, and the Law
United States Senate

Josh Hawley
Ranking Member
Subcommittee on Privacy, Technology, and the Law
United States Senate