ABIGAIL SPANBERGER
7TH DISTRICT, VIRGINIA

Congress of the United States
House of Representatives
Washington, DC 20515

July 23, 2024

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

Dear Mr. Stankey,

On July 12, 2024, AT&T revealed that hackers stole customer data — including phone numbers, call duration times, and location data stored on the third-party cloud platform Snowflake — for all customers who made calls or sent texts from May 1, 2022 to October 31, 2022, and some customers who had service on January 2, 2023. The cyberattack also compromised the data of friends, colleagues, and loved ones in contact with these AT&T customers, irrespective of their network provider, and potentially the data of mobile virtual network operators like Boost Mobile and Cricket Wireless who use AT&T's infrastructure — a massive breach of security, privacy, and peace of mind.

I'm writing to express my grave concern about this hack, and to better understand the steps your company is taking to mitigate harm and better secure customer data going forward. Unfortunately, Virginians stand to be especially harmed by the attack. My district is home to thousands of military personnel, intelligence officers, and other national security professionals whose ability to complete their missions — and their personal safety — could be at risk because of this hack.

Before coming to Congress, I served as a case officer at the Central Intelligence Agency. Throughout my tenure at CIA, it was my job to maintain tight security of my contacts for the safety of my assets, my colleagues, and myself. This stolen customer data — which includes valuable call records, records of text message exchanges, and personally identifying information — becomes especially perilous when acquired or purchased by foreign adversaries. When armed with this valuable information, maligned governments — like the Russian Kremlin and the Chinese Communist Party — and state-sponsored intelligence agencies could trace these phone numbers back to their owners to expose contacts, sensitive communications networks, and even the precise locations of callers.

Beyond the national security community, individual Americans are more vulnerable after these data breaches. Year after year, the Federal Bureau of Investigations (FBI) has reported an increase in the number of complaints it receives about personal data breaches — often enabled by the kind of data stolen from your company.[1] While I appreciate AT&T's public statement and efforts to notify affected customers — and that your company is continuing to investigate the full impact of the breach — I'm requesting additional information about your security plans and practices going forward:

- In the future, how will your company safeguard the data of the millions of customers who trust and use your product?

- Do you plan to change data retention protocols to diminish risk?

[1] Federal Bureau of Investigation. *2022 Internet Crime Report*. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

ABIGAIL SPANBERGER
7TH DISTRICT, VIRGINIA

Congress of the United States
House of Representatives
Washington, DC 20515

- Snowflake has launched features, like multifactor authentication, to bolster security. What steps has your company taken to evaluate and coordinate with Snowflake to prevent a similar breach in the future?

- Given the nature of the data that was breached and the possibility for it to be used for phishing using social engineering tactics, will your company offer fraud monitoring services, free of charge, to affected parties?

- Though investigations into the perpetrator are ongoing, press reports indicate your company paid the alleged hacker over $370,000 to delete the stolen data[2] — do you have any reason to believe any of the data remain vulnerable or were sold to a third party?

- News reports indicate a threat actor "claimed to have unlawfully accessed and copied AT&T call logs," alerting AT&T to the breach on April 19, 2024.[3] However, AT&T's recent regulatory filing stated that the hacker had successfully exfiltrated files as early as April 14, 2024, and continued until April 25, 2024. Given the length of time it took your company to resolve the breach after learning of it, and the hacker voluntarily alerting the company to the breach, do you have any reason to believe there may be other, unrelated compromises of which you are not yet aware?

- How did AT&T's incidence response plan help to mitigate the damage done by the threat actor, and why did it take six days to secure the breach access point?

- What resources can Congress and the broader United States federal government provide to assist you and peer telecommunications companies in preventing, thwarting, and disincentivizing future attacks?

I look forward to reviewing your responses and thank you for your timely attention to this request.

Sincerely,

Abigail D. Spanberger
Member of Congress

[2] https://www.wired.com/story/atandt-paid-hacker-300000-to-delete-stolen-call-records/
[3] https://www.cnn.com/2024/07/12/business/att-customers-massive-breach/index.html