

ONE HUNDRED EIGHTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-3641
Minority (202) 225-2927

October 10, 2024

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

Dear Mr. Stankey,

We are concerned by the recent reports of a massive breach of AT&T, Verizon, and Lumen's communications networks by Chinese hackers.¹ These types of breaches are increasing in frequency and severity, and there is a growing concern regarding the cybersecurity vulnerabilities embedded in U.S. telecommunications networks. The Committee needs to understand better how this incident occurred and what steps your company is taking to prevent future service disruptions and secure your customers' data.

On October 5th, *The Wall Street Journal* reported U.S. broadband providers were breached by a Chinese government-tied hacker organization.² The attack appears to be geared towards intelligence collection, and Chinese hackers potentially accessed vulnerable information including court-authorized network wiretapping requests and internet traffic.³ A person familiar with the attack said "the U.S. government considered the intrusions to be historically significant and worrisome."⁴ This is extremely alarming for both economic and national security reasons.

In an age where Americans rely heavily on your services for communication and connectivity, the integrity of your networks is paramount. It is vital that cybersecurity protocols are enhanced to better protect American's data against increasingly sophisticated attacks especially from our foreign adversaries.

¹ China hacked major U.S. telecom firms in apparent counterspy operation, *The Washington Post* (Oct. 6, 2024), <https://www.washingtonpost.com/national-security/2024/10/06/salt-typhoon-china-espionage-telecom/>

² U.S. Wiretap Systems Targeted in China-Linked Hack, *The Wall Street Journal* (Oct. 5, 2024), <https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b>

³*Id.*

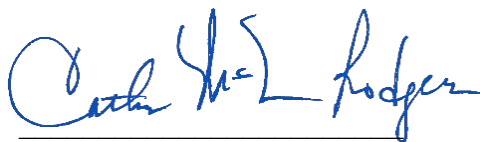
⁴*Id.*

We therefore request a briefing before October 18, 2024, to understand how these breaches occurred and what steps your company has taken to fortify the security of your network. We also request the following information by October 18, 2024:

1. When and how did AT&T become aware that its network had been breached?
2. What law enforcement entities, if any, did AT&T contact upon learning that the breach occurred?
3. What steps has AT&T taken to notify customers of the breach and what is AT&T doing to assist customers whose data has been compromised?
4. Has AT&T conducted thorough investigations to identify vulnerabilities in its network and implement corrective measures?
5. What steps has AT&T taken to address security vulnerabilities since each breach?
6. What information was the hacker able to acquire as a result of this breach?
7. What legislative actions should Congress take to assist AT&T in protecting your networks and your customers' data?
8. Are there any other issues or sensitivities the Committee should be aware of with respect to this incident?

Please contact the Committee Majority staff at (202) 225-3641 to schedule the briefing. Thank you for your attention to this urgent matter.

Sincerely,



Cathy McMorris Rodgers
Chair
House Energy and Commerce Committee



Frank Pallone
Ranking Member
House Energy and Commerce
Committee

Mr. John T. Stankey

Page 3

Handwritten signature of Robert E. Latta in blue ink, written over a horizontal line.

Robert E. Latta

Chair

Subcommittee on Communications
and Technology

Handwritten signature of Doris Matsui in blue ink, written over a horizontal line.

Doris Matsui

Ranking Member

Subcommittee on Communications
and Technology