United States Senate
WASHINGTON, DC 20510

August 2, 2024

VIA ELECTRONIC TRANSMISSION

The Honorable Jeff Zients
Chief of Staff
The White House

Dear Mr. Zients:

According to an AT&T Securities and Exchange Commission (SEC) filing, AT&T was the victim of a data breach from April 14-25, 2024.[1] The filing stated a cyber-actor unlawfully "accessed and copied…records of calls and text messages of nearly all of AT&T's wireless customers" that occurred from May 1, 2022, to October 31, 2022, and on January 2, 2023.[2] The records identify the telephone numbers that an AT&T or mobile virtual network operator (MVNO) number interacted with, including telephone numbers of AT&T customers and customers from other carriers, counts of the interactions, and aggregate call duration for a day or month.[3] Though the data does not contain the content of calls and texts, it does contain other data.[4] This breach impacted over 90 million people, potentially including data from our federal agencies, and is cause for serious alarm.[5]

I've previously raised concerns about the need to protect our nation's cybersecurity and U.S. critical infrastructure.[6] I wrote to the Cybersecurity and Infrastructure Security Agency

[1] AT&T Inc., Annual Report (Form 8-K) (July 12, 2024).
[2] *Id.*
[3] *Id.*
[4] *Id.* ("there are often ways, using publicly available online tools, to find the name associated with a specific telephone number"); *see also* Patrick Smith, et al., *AT&T says hackers stole records of nearly all cellular customers' calls and texts*, NBC NEWS (July 12, 2024), https://www.nbcnews.com/news/us-news/t-says-hackers-stole-records-nearly-cell-customers-calls-texts-rcna161507 (metadata is "considered highly sensitive, especially when collected and analyzed at large scales to reveal patterns and connections between people").
[5] Alyssa Lukpat, *What AT&T Customers Need to Know About the Massive Hack, Data Breach*, WALL STREET JOURNAL (July 12, 2024), https://www.wsj.com/business/telecom/att-data-breach-hack-customers-explained-b39438dd; David DiMolfetta, *Dozens of federal agencies' call data potentially exposed in AT&T breach*, NEXTGOV (July 12, 2024), https://www.nextgov.com/cybersecurity/2024/07/dozens-federal-agencies-call-data-potentially-exposed-t-breach/398005/.
[6] Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (July 3, 2024), https://www.grassley.senate.gov/imo/media/doc/grassley_to_cisa_-_cyberattack.pdf; Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (Mar. 4, 2024), https://www.grassley.senate.gov/imo/media/doc/grassley_to_cisa_-_critical_infrastructure.pdf; *see also* Press Release, Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, Grassley: Federal Agencies Must Stop 'Dragging Their Feet' On Bolstering Cybersecurity Defense

(CISA) on March 4, 2024, regarding its decision to prioritize misinformation and disinformation over the protection of our nation's critical infrastructure.[7] On April 8, 2024, I also wrote letters to seven of the Sector Risk Management Agencies responsible for overseeing our nation's critical infrastructure to highlight the threat of cyberattacks on our critical infrastructure sectors, including the communications sector.[8] Last month, I again wrote to CISA regarding a recent cyberattack, which released "potential unauthorized" information on its internal agency processes and "critical information about the operations of our U.S. infrastructure."[9] It is imperative that our federal agencies work with private industry to ensure all data and critical infrastructure is safe and secure.

Accordingly, so Congress may conduct objective and independent oversight concerning the April 2024 AT&T data breach, please provide answers to the following no later than August 16, 2024:

1. Was the EOP impacted by the April 14-25 AT&T data breach?

    a. If so, provide a full and complete list of all departments, organizations, and individuals that were impacted or potentially impacted.

        i. Has the EOP notified these entities about the data breach and that their information could be at risk of future misuse?

    b. If so, when did the EOP become aware of the data breach?

    c. If so, has the EOP communicated with AT&T or other federal authorities about the April 14-25 data breach? Provide all records.[10]

    d. If so, what specific steps is the EOP taking both internally and with AT&T to secure its data from future breaches and cyberattacks? Provide all records.

(Apr. 8, 2024), https://www.grassley.senate.gov/news/news-releases/grassley-federal-agencies-must-stop-dragging-their-feet-on-bolstering-cybersecurity-defense.

[7] Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (Mar. 4, 2024), *supra* note 6.

[8] Grassley: Federal Agencies Must Stop 'Dragging Their Feet' On Bolstering Cybersecurity Defense, *supra* note 6.

[9] Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (July 3, 2024), *supra* note 6.

[10] "Records" include any written, recorded, or graphic material of any kind, including letters, memoranda, reports, notes, electronic data (emails, email attachments, and any other electronically created or stored information), calendar entries, inter-office communications, meeting minutes, phone/voice mail or recordings/records of verbal communications, and drafts (whether they resulted in final documents).

Thank you for your prompt review and responses. If you have any questions, please contact Tucker Akin on my Committee staff at (202) 224-0642.

Sincerely,

Charles E. Grassley
Ranking Member
Committee on the Budget