

United States Senate
WASHINGTON, DC 20510

August 2, 2024

VIA ELECTRONIC TRANSMISSION

Mr. John Stankey
Chief Executive Officer
AT&T

Dear Mr. Stankey:

From April 14-25, 2024, a cyber-actor accessed and copied records relating to calls and text messages of nearly every AT&T customer that occurred from May 1, 2022, to October 31, 2022, and on January 2, 2023.¹ According to an AT&T Securities and Exchange Commission (SEC) filing, AT&T did not learn of the data breach until April 19, 2024.² While the records reportedly do not contain the content of calls and texts, they contain other data, including telephone numbers, counts of interactions, and aggregate call duration for a day or month.³ This breach placed the data of over 90 million people at risk, potentially including records from federal agencies.⁴ AT&T must explain how this data breach happened and what is being done to ensure that it does not place American data at risk again.

I've previously raised concerns about the need to protect our nation's cybersecurity and U.S. critical infrastructure.⁵ I wrote to the Cybersecurity and Infrastructure Security Agency (CISA) on March 4, 2024, regarding its decision to prioritize misinformation and disinformation

¹ AT&T Inc., Annual Report (Form 8-K) (July 12, 2024).

² *Id.*

³ *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").

⁴ 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/>.

⁵ 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 (Apr. 8, 2024), <https://www.grassley.senate.gov/news/news-releases/grassley-federal-agencies-must-stop-dragging-their-feet-on-bolstering-cybersecurity-defense>.

over the protection of our nation's critical infrastructure.⁶ 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.⁷ 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."⁸ As a steward of federal government and American citizens' data, it is crucial that AT&T ensures all data is safe and secure from bad actors.

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. How did AT&T discover the data breach on April 19, 2024? Why did it take five days for AT&T to detect this data breach? Provide all records from AT&T's internal investigation into this incident.⁹
2. Why did the data breach continue for five days after AT&T learned about the unauthorized access to its files? Provide copies of AT&T's policies and protocols regarding data breaches and cyberattacks in place at the time of this incident.
3. When did AT&T alert federal authorities regarding the data breach? Provide all records.
4. How many federal agencies, departments, or organizations were impacted or potentially impacted by the April 14-25 data breach? Has AT&T communicated with all of these entities? If not, why not?
5. Why did AT&T wait nearly three months to make a public announcement about this data breach?
6. Was AT&T aware of any potential vulnerabilities before the April 14-25 data breach? If so, what measures did AT&T take to secure customers' data? Provide all records.
7. What specific steps is AT&T taking to secure its data from future data breaches and cyberattacks? Provide all records.

⁶ 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 5.

⁷ Grassley: *Federal Agencies Must Stop 'Dragging Their Feet' On Bolstering Cybersecurity Defense*, *supra* note 6.

⁸ 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 5.

⁹ "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,

A handwritten signature in blue ink that reads "Chuck Grassley". The signature is written in a cursive, flowing style.

Charles E. Grassley
Ranking Member
Committee on the Budget