CAROLYN B. MALONEY
CHAIRWOMAN

ONE HUNDRED SIXTEENTH CONGRESS

JAMES COMER
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5051
MINORITY (202) 225–5074
https://oversight.house.gov

August 11, 2020

Mr. Jack Dorsey
Chief Executive Officer
Twitter, Inc.
355 Market Street, Suite 100
San Francisco, CA 94103

Dear Mr. Dorsey:

Thank you for providing a briefing to the Committee last week regarding the July 15, 2020 cyberscam that took place on Twitter. Your responsiveness to the Committee has been swift, and Twitter's desire to publicize information regarding the security breach is commendable. Unfortunately, during a briefing with Committee staff, Twitter was unable to answer several basic questions outlined in my July 16, 2020 letter to you, and the briefing raised many more questions than answers.

The breach of Twitter's security last month was the third major disruption in recent memory. In 2017, the President's personal Twitter feed was deleted by a disgruntled employee on his last day at Twitter.[1] Last year, your personal Twitter feed was breached because, according to your staff, the phone company had a "security oversight."[2] Finally, last month dozens of high-profile Twitter accounts were accessed by an individual who is not even a legal adult.[3]

Though the sheer number of security breaches of high-profile Twitter accounts is astonishing, perhaps more astonishing is the relative unsophisticated nature of each breach. Such easy access to Twitter's internal controls is emblematic of the cavalier nature with which the company takes its security. To wit, Twitter told the Committee its employees were the real victims of last month's attacks—not those whose accounts were compromised or who lost money as a result of the cyberscam.[4]

---

[1] Mike Isaac and Daisuke Wakabayashi, *Twitter's Panic After Trump's Account Is Deleted Caps a Rough Week*, N.Y. TIMES, Nov. 3, 2017, available at https://www.nytimes.com/2017/11/03/technology/trump-twitter-deleted.html.
[2] Brian Barrett, *How CEO Jack Dorsey's Account Was Hacked*, WIRED, Aug. 30, 2019, available at https://www.wired.com/story/jack-dorsey-twitter-hacked/.
[3] Martin Matishak, *Florida teen, 2 others arrested over massive Twitter breach*, POLITICO, July 31, 2019, available at https://www.politico.com/news/2020/07/31/twitter-hack-florida-teen-arrested-389799.
[4] Twitter briefing to H. Comm. on Oversight and Reform, July 30, 2020 [hereinafter "Twitter briefing"].

Even more alarming is Twitter's response to last month's breach. Twitter blamed the breach on individuals exploiting employees "working from home."[5] Yet, despite the fact Twitter employees may be working from home forever,[6] your staff said Twitter is "not in a post-mortem state to talk about changes" the company is thinking about making regarding additional security measures.[7] Even though you have acknowledged Twitter "fell behind, both in our protections against social engineering of our employees and restrictions on our internal tools,"[8] Twitter laid out for the Committee no plans to address either of these moving forward.

Twitter emphasized to the Committee it is a not a large organization, with only 4,000 employees, and had "resource constraints."[9] But, Twitter claims, with over 160 million average daily users its users require a certain level of customer service. As such, according to one estimate, nearly 1,500 staff and contractors—a number equaling roughly 40% of Twitter's entire workforce—have the ability to "reset accounts, review user breaches and respond to potential content violations." This access serves as a "starting point to snoop on or even hack an account."[10]

During last week's briefing, Twitter was unable to answer even basic questions about employee access to user accounts and Twitter's arrangement with its contractors. Particularly concerning to the Committee is the possibility Twitter employees and contractors have access to user IP addresses and possibly the locations of physical devices logged into a user's Twitter app profile. If true, any possible abuse or breach of this access has grave implications given that hundreds of world leaders, business elites, and other high-profile persons of interest frequently use Twitter to communicate with the public. The damage a malicious nation-state could do if they were to devote resources towards compromising Twitter's security could be grave.

Therefore, please provide the following documents to the Committee no later than 5:00 p.m. on August 18, 2020:

1) A copy of the recent training provided to all Twitter employees in the wake of last month's breach;

2) A copy of Twitter's anti-phishing guidance in place prior to last month's breach;

---

[5] *Id.*
[6] Brian Fung, *Twitter will let some employees work from home 'forever,'* CNN, May 12, 2020, available at https://www.cnn.com/2020/05/12/tech/twitter-work-from-home-forever/index.html.
[7] Twitter briefing.
[8] Joseph Menn et al., *Exclusive: More than 1,000 people at Twitter had ability to aid hack of accounts*, REUTERS, July 23, 2020, available at https://www.reuters.com/article/us-twitter-cyber-access-exclusive/exclusive-more-than-1000-people-at-twitter-had-ability-to-aid-hack-of-accounts-idUSKCN24O34E#:~:text=On%20a%20call%20to%20discuss,tools%2C%E2%80%9D%20Dorsey%20told%20investors.
[9] Twitter briefing.
[10] Jordan Robertson et al., *Twitter's Security Woes Included Broad Access to User Accounts*, BLOOMBERG, July 27, 2020, available at https://www.bloomberg.com/news/articles/2020-07-27/twitter-s-security-woes-included-broad-access-to-user-accounts.

3) A list of all employees and contractors who have the ability to reset Twitter user passwords and/or have user level access to user accounts;

4) A description of, and as available a copy of, any internal policies and guidelines for granting a Twitter employee or contractor the ability to reset user passwords and/or have user level access to user accounts;

5) A copy of Twitter's protocols outlining the company's response to security incidents; and

6) A copy of Twitter's guidance regarding telework that applies to Twitter employees, including any additional security measures taken in the wake of last month's breach.

Thank you in advance for your cooperation with this matter.

Sincerely,

James Comer
Ranking Member

cc: The Honorable Carolyn Maloney, Chairwoman