



One Hundred Seventeenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

August 25, 2022

Mr. Parag Agrawal
Chief Executive Officer
Twitter, Inc.
1355 Market Street
San Francisco, CA 94103

Dear Mr. Agrawal:

We write to express our deep concern about disturbing whistleblower allegations raised by Twitter’s former head of security regarding poor security and privacy practices at Twitter and the company’s preparedness for the 2022 midterm elections.

In a complaint filed with the Securities and Exchange Commission, Federal Trade Commission, and Department of Justice earlier this week, Twitter’s former head of security, Peiter “Mudge” Zatkó, identified “egregious deficiencies” in Twitter’s security program that were brought to the company’s attention, but nevertheless ignored.¹ According to the complaint, Mr. Zatkó tried to warn Twitter about widespread vulnerabilities in its servers and company devices that, if exploited, could result in massive data loss and bring operations to a halt. Mr. Zatkó asserts he tried to shed new light on known problems Twitter had failed to remedy for over a decade. For instance, the complaint alleges that almost half of Twitter’s 7,000 employees retain overly broad, unmanaged access to core company systems and data – despite the practice causing years of embarrassing, costly, and sometimes dangerous² security incidents. Mr. Zatkó also points to multiple instances where Twitter executives obfuscated and mischaracterized information to Congress, regulators, and its own board – and may have even bowed to pressure from foreign governments to put their

¹ Joseph Menn, Elizabeth Dwoskin, and Cat Zakrewski, “Former security chief claims Twitter buried ‘egregious deficiencies,’” *Washington Post*, Aug. 23, 2022, <https://www.washingtonpost.com/technology/interactive/2022/twitter-whistleblower-sec-spam/> (reporting on redacted SEC complaint, *Re: Protected Disclosures of Federal Trade Commission Act Violations, Material Misrepresentations and Omissions, and Fraud by Twitter, Inc. and CEO Parag Agrawal*, available at <https://www.washingtonpost.com/technology/interactive/2022/twitter-whistleblower-sec-spam/?document=undefined>).

² See generally, Julian Borger, “Ex-Twitter employee found guilty of spying on Saudi dissidents,” *The Guardian*, Aug. 9, 2022, <https://www.theguardian.com/us-news/2022/aug/09/twitter-saudi-arabia-dissident-spying> (a former Twitter employee “used his position at Twitter to find personal details identifying critics of the Saudi monarchy who had been posting under anonymous Twitter handles, and then supplying the information to Prince Mohammed’s aide Bader al-Asaker”).

operatives on the company's payroll.³ If any of these allegations are true, Twitter has a staggering security to-do list.

Unfortunately, Twitter's to-do list for the 2022 midterm elections is no less daunting. In research commissioned by Mr. Zatko during his time at Twitter, the misinformation consulting firm Alethea Group described Twitter's site integrity team as grossly under-resourced and under-staffed, with only two employees dedicated to combating misinformation in 2021.⁴ The group reportedly lacked the technical tools, engineers, and language proficiencies to identify and manage misinformation effectively. The researchers concluded that "organizational siloing, a lack of investment in critical resources, and reactive policies and processes have driven Twitter to operate in a constant state of crisis that does not support the company's broad mission of protecting authentic conversation."⁵

American democracy is at an inflection point, and there is no question that the 2022 midterms and the 2024 presidential elections will test our institutions. It is worth remembering how we got here. In 2016, social media companies were caught flat-footed when Russian operatives used platforms like Twitter to carry out a widespread disinformation campaign to influence the results of the presidential election. By the 2020 election, the threat of disinformation had evolved, but it persisted. At that time, Twitter and other platforms assured Congress that they had invested heavily in putting people, plans, and policies in place to protect against election misinformation. As you know, that election was followed by an unprecedented, violent attack on our Nation's Capitol, fueled by the lie spread rampantly on social media that the 2020 election had been stolen.

Twitter plays a unique role in our information and political ecosystems. Security flaws that put users' sensitive personal data within easy reach of a hacker looking to take control of a high-profile account or a foreign dictator looking for information on dissidents are nothing short of a threat to national security. If substantiated, the whistleblower allegations demonstrate a pattern of willful disregard for the personal data of Twitter users and the integrity of the platform.

Pursuant to Rule X(3)(g) of Rule XI of the Rules of the House of Representatives, I request you provide a written response to the following questions, and whatever supplementary information you deem responsive, by September 8, 2022:

1. Please describe, with specificity, the extent to which Twitter has or has not resolved the security flaws identified in Mr. Zatko's complaint – including with respect to (1) out-of-date, vulnerable servers; (2) deficiencies in the company's vulnerability and patch management program; and (3) limiting privileges and access controls for employees and contractors at Twitter?

³ Menn, *supra* n.1 ("complaint says he believed the Indian government had forced Twitter to put one of its agents on the payroll, with access to user data at a time of intense protests in the country"); *See also*, Munsif Vengattil and Fanny Potkin, "India forced Twitter to put agent on payroll, whistleblower says," Reuters, Aug. 23, 2022, <https://www.reuters.com/world/india/india-forced-twitter-put-agent-payroll-whistleblower-says-2022-08-23/>.

⁴ Rebecca Kern, "Twitter's newest crisis deepens its midterms morass," *POLITICO*, Aug. 23, 2022, <https://subscriber.politicopro.com/article/2022/08/twitter-zatko-cybersecurity-whistleblower-election-2022-00053416?source=email> (citing draft report by Alethea Group, *Twitter's Efforts Against Propaganda*, available at <https://www.washingtonpost.com/technology/interactive/2022/twitter-whistleblower-sec-spam/?document=undefined>).

⁵ *Id.*

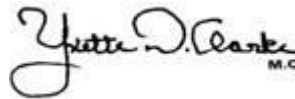
2. Please describe any actions taken in response to any warnings or recommendations Twitter received from Mr. Zatkan, both during his tenure with the company and following his departure, in response to the complaint and/or public reporting surrounding the complaint?
3. What is Twitter's plan to prioritize, remedy, and address security deficiencies raised in Mr. Zatkan's complaint? How will Twitter prioritize security upgrades necessary to combat disinformation in time for the upcoming midterm elections?
4. Earlier this month, Twitter announced that it would be reinstating its 2020 election integrity rules for the 2022 midterms.⁶ Has this policy changed since 2020, and if so, how? What lessons did Twitter learn in its execution of these rules during the 2020 election, and how does Twitter plan to incorporate those lessons in 2022 and 2024?
5. The Alethea report indicated that, within Twitter's Site Integrity team, only two employees were dedicated to misinformation in 2021. Is that accurate? How many employees are dedicated to Twitter's misinformation mission now? How many dedicated employees does Twitter currently have working directly on combatting election-related misinformation and disinformation? What percentage of Twitter's annual revenue is devoted specifically to addressing election misinformation?
6. Is the Alethea report provided by Mr. Zatkan authentic? Are its findings accurate? If not, please explain.
7. How is Twitter working with the Cybersecurity and Infrastructure Security Agency (CISA) to address security deficiencies like the ones identified in the complaint and to prepare for the upcoming midterm election? Has Twitter ever requested or received any cybersecurity resources or services that CISA makes available upon request?
8. Moving forward, will Twitter commit to voluntarily reporting any serious cybersecurity incidents it experiences to CISA to improve CISA's understanding of the tactics, techniques, and procedures of our adversaries and other hackers?

Thank you for your attention to this request.

Sincerely,



BENNIE G. THOMPSON
Chairman



YVETTE D. CLARKE
Chairwoman
Subcommittee on Cybersecurity,
Infrastructure Protection, & Innovation

⁶ Sheila Dang, "Twitter plan to fight midterm misinformation falls short, voting rights experts say," Reuters, Aug. 11, 2022, <https://www.reuters.com/world/us/twitter-reintroduces-election-misinformation-rules-ahead-us-midterms-2022-08-11/>.

