United States Senate
WASHINGTON, DC 20510

August 23, 2022

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chair Khan,

I write to express serious concern over recent whistleblower disclosures regarding Twitter's data security practices and to encourage the Federal Trade Commission (FTC) to investigate any breach of Twitter's 2011 consent decree with the Commission or violations of our consumer protection laws.

According to disclosures and evidence provided by Peiter "Mudge" Zatko, a highly-respected cybersecurity expert who served as Twitter's Security Lead from 2020 to 2022, Twitter executives allegedly failed to address significant security vulnerabilities, neglected the mishandling of personal data, and ignored known privacy risks to users for more than a decade. These troubling disclosures paint the picture of a company that has consistently and repeatedly prioritized profits over the safety of its users and its responsibility to the public, as Twitter executives appeared to ignore or hinder efforts to address threats to user security and privacy.

Twitter's security failures are notorious. As recently as this month, Twitter confirmed that a vulnerability led to the disclosure of private information of more than 5 million accounts, a lapse that Twitter acknowledged could be used by repressive regimes to track down dissidents.[1] That disclosure follows recent high profile breaches involving an employee spying on dissidents on behalf of the Saudi government and the hijacking by a scammer of over a hundred prominent accounts, including those of then presidential candidate Biden and former President Obama.[2]

---

[1] "An incident impacting some accounts and private information on Twitter." Twitter. August 5, 2022. https://privacy.twitter.com/en/blog/2022/an-issue-affecting-some-anonymous-accounts

[2] "Former Twitter Employee Found Guilty of Acting as an Agent of a Foreign Government and Unlawfully Sharing Twitter User Information." Department of Justice. August 10, 2022. https://www.justice.gov/opa/pr/former-twitter-employee-found-guilty-acting-agent-foreign-government-and-unlawfully-sharing
"A Brazen Online Attack Targets V.I.P. Twitter Users in a Bitcoin Scam." New York Times. July 15, 2017. https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html

These serious breaches alone demonstrate that Twitter's security failures present a significant national security risk that has been exploited by criminals and foreign governments.

Mr. Zatko's disclosures appear to show that Twitter created the conditions for these breaches through failing to meaningfully restrict, protect, monitor, and account for access to consumers' data. Specifically, Mr. Zatko alleges that Twitter suffered from an "anomalously high rate of security incidents" due to its failures to limit access to databases, servers, and personal data.[3] He also contends that Twitter had not taken basic measures to apply security updates and track vulnerabilities, including the Log4j vulnerability the FTC warned companies to address.[4] Those risks were reportedly compounded by indications that another foreign government had forced the company to hire particular employees, which created concerns of more spying on Twitter users similar to the Saudi case. According to Mr. Zatko, these unaddressed risks led him to fear that "Twitter could suffer an Equifax-level hack."[5]

The Federal Trade Commission first put Twitter on notice over its poor data security practices a decade ago, bringing an enforcement action that cited lax internal controls and the hijacking of accounts (including that of President Obama).[6] As a part of the consent decree that Twitter agreed to, the company was required to establish and maintain a comprehensive information security program to protect consumer data and privacy.

Mr. Zatko's disclosures indicate that Twitter management has failed to honor the terms of the consent decree. In fact, Mr. Zatko alleges that Twitter executives were aware that the company has never been in compliance with the consent decree and was not on track to come into compliance. I am especially concerned by allegations that Twitter executives were not only aware of specific risks and recommendations to address those vulnerabilities, but that they also failed to act and interfered with attempts to inform the Board of Directors.

While I appreciate that, this May, the Commission brought an enforcement action against Twitter for its deceptive misuse of account information for advertising, that case does not fully address the repeated known security lapses and allegations related to the FTC's existing consent decree. If the Commission does not vigorously oversee and enforce its orders, they will not be taken seriously and these dangerous breaches will continue.

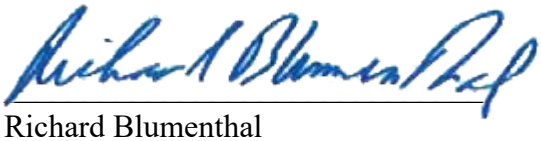
---

[3] Zatko SEC Disclosure.
[4] "FTC warns companies to remediate Log4j security vulnerability." Federal Trade Commission. January 4, 2022. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability
[5] Zatko SEC Disclosure.
[6] "Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program." Federal Trade Commission. June 24, 2010. https://www.ftc.gov/news-events/news/press-releases/2010/06/twitter-settles-charges-it-failed-protect-consumers-personal-information-company-will-establish

I urge the Commission to investigate the allegations and information provided in Mr. Zatko's whistleblower complaint, and to bring enforcement actions against any breaches of its consent decree or business practices that are unfair or deceptive, including bringing civil penalties and imposing liability on individual Twitter executives where appropriate.

Thank you for your attention to this important matter.

Sincerely,



Richard Blumenthal
Chair
Subcommittee on Consumer Protection,
Product Safety, and Data Security
United States Senate