United States Senate

August 23, 2022

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

The Honorable Merrick B. Garland
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530

Dear Chair Khan and Attorney General Garland,

I write with significant concerns about Twitter's security practices. According to Peiter Zatko, Twitter's former head of security, Twitter has systematically and repeatedly failed to take basic security measures to protect its user data and has misled investors, regulators, and the public about the strength of its security systems.[1] These alarming allegations suggest that Twitter has again flagrantly violated its 2011 consent decree with the Federal Trade Commission (FTC), after just recently settling with the Department of Justice (DOJ) and FTC for violating that order. I urge the federal government to immediately investigate these charges and, if necessary, take swift action to enforce the 2011 agreement, hold Twitter accountable for any illegal activity, and protect the data of Twitter's users.

Twitter's poor security measures are, unfortunately, nothing new. Over a decade ago, the FTC issued a complaint against the upstart social media company, alleging that Twitter misled its users about its security features.[2] For example, while Twitter's privacy policy declared that it "employ[ed] administrative, physical, and electronic measures designed to protect [user] information,"[3] in fact, from July 2006 to July 2009, almost every Twitter employee could exercise administrative control over Twitter's system, including accessing users' nonpublic tweets and account information.[4] Subsequently, hackers breached Twitter's security measures and gained control over its system on at least two occasions during that period.[5] In a 5-0 decision, the FTC settled its complaint against Twitter and required the company to cease misleading users about its security policies. The consent agreement also required Twitter to implement a comprehensive security program to protect user data and guard against malicious

[1] Complaint, Peiter Zatko (July 6, 2022), https://www.washingtonpost.com/technology/interactive/2022/twitter-whistleblower-sec-spam/whistleblower_disclosure.pdf (hereinafter "Zatko Complaint").
[2] *In re Twitter, Inc.*, C-4316, 151 F.T.C. 162 (Mar. 11, 2011) (Administrative Complaint).
[3] *Id.* at ¶ 10.
[4] *Id.* at ¶ 7.
[5] *Id.* at ¶ 12.

threats.[6] As David Vladeck, the then-director of the FTC's Bureau of Consumer Protection, said in a statement at the time, "When a company promises consumers that their personal information is secure, it must live up to that promise."[7] Twitter failed to live up to that promise.

This embarrassing episode should have forced Twitter to swiftly and effectively update its security policies. But according to Zatko, Twitter failed to take such action. In fact, Twitter — now a publicly traded company valued at more than $30 billion — appears to have, at best, paid lip service to complying with the FTC settlement and, at worse, effectively disregarded it altogether. Zatko's complaint details a long list of concerning conduct. For example, roughly 30 percent of Twitter employees' laptops allegedly block automatic software updates, which often include critical security updates.[8] According to Zatko, Twitter also continued to allow about half of its 10,000 employees "access to sensitive live production systems and user data" — the deficient internal control that led to the FTC's 2011 complaint.[9] Twitter also allegedly lacks redundancy measures to maintain its systems in the event of "even a minor overlapping data center failure,"[10] and knowingly hired agents of the Indian government, giving them — and therefore the Indian government — access to user data.[11] And when Zatko attempted to inform the Board of Directors about these security issues, he was apparently instructed not to do so.[12] This lax culture of security was not unusual at Twitter, according to Zatko, who joined Twitter in 2020. Other experienced employees allegedly told him "unequivocally" that "Twitter had never been in compliance with the 2011 FTC Consent Order, and was not on track to ever achieve full compliance."[13]

Unsurprisingly, then, Twitter has continued to suffer embarrassing security incidents and face ongoing scrutiny for misleading users and regulators. For example, Twitter has proven unable to protect its highest-profile users. In 2017, a company employee deactivated for 11 minutes then-President Donald Trump's account,[14] and in July 2020, hackers simultaneously accessed Twitter accounts owned by Joe Biden, Barack Obama, Kanye West, Bill Gates, and Elon Musk.[15] Moreover, in May, Twitter agreed to pay $150 million to settle allegations by the

---

[6] Press Release, Federal Trade Commission, FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information (Mar. 11, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/03/ftc-accepts-final-settlement-twitter-failure-safeguard-personal-information-0.

[7] Press Release, Federal Trade Commission, Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program (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.

[8] Zatko Complaint, *supra* note 1, at ¶ 46(b)(ii).

[9] *Id*. at ¶ 46(b)(i).

[10] *Id*. at ¶ 46(c)(iii).

[11] *Id*. at ¶ 72(a).

[12] *Id.* at ¶ 3.

[13] *Id*. at ¶ 46.

[14] Hayley Tsukayama, Rachel Siegel & J. Freedom du Lac, *Rogue Twitter employee deactivated Trump's personal account on last day on the job, company says*, WASH. POST (Nov. 3, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/11/02/trumps-twitter-account-was-temporarily-deactivated-due-to-human-error/.

[15] Sheera Frenkel et al., *A Brazen Online Attack Targets V.I.P. Twitter Users in a Bitcoin Scam*, N.Y. TIMES (July 15, 2020), https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html.

Department of Justice, together with the FTC, that the company violated the 2011 FTC settlement by utilizing its users' telephone numbers and email addresses for marketing after telling them that Twitter would only use that personal information for security purposes.[16]

Taken together, Zatko's allegations, the DOJ and FTC complaints, and the repeated security incidents illustrate a company that prioritizes profit over users and has allowed a culture of impunity to reign supreme. Like other powerful online platforms, Twitter collected user data with deficient security measures, settled with the FTC for misleading users, and then continued operating with few changes. This blithe disregard for user data and FTC settlements cannot stand. I strongly urge the federal government to investigate Zatko's claims and, if necessary, take strong and swift action against Twitter to ensure Twitter user data is properly protected.

Thank for your work on this critical matter.

Sincerely,

Edward J. Markey
United States Senator

[16] Press Release, Department of Justice, Twitter Agrees with DOJ and FTC to Pay $150 Million Civil Penalty and to Implement Comprehensive Compliance Program to Resolve Alleged Data Privacy Violations (May 25, 2022), https://www.justice.gov/opa/pr/twitter-agrees-doj-and-ftc-pay-150-million-civil-penalty-and-implement-comprehensive.