



Office of the Chair

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

February 21, 2024

The Honorable Jim Jordan
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Jordan:

I am writing in further response to your April 12, 2023, letter requesting documents and information related to Twitter, in an additional effort to be responsive to your request. This letter addresses your questions regarding the Federal Trade Commission's investigation of potential third-party access to the information of Twitter users. It also addresses your inquiry regarding the FTC's review of Twitter's numerous employee terminations and resignations.

The FTC's mission is protecting Americans from unfair methods of competition and unfair or deceptive practices. Safeguarding Americans' privacy and personal data are bedrocks of the FTC's consumer protection mandate.

Businesses subject to FTC consent orders are legally obliged to abide by those commitments. FTC staff systematically monitor compliance with all FTC consumer protection orders. As part of that process, compliance staff are assigned to each matter. The compliance staff review and analyze the respondent's or defendant's compliance reports and other information, such as media reports and consumer complaints, and conduct further reviews and inquiry as appropriate.

Consistent with the FTC's established monitoring practices, the FTC has been monitoring Twitter's compliance with the 2022 FTC consent decree (the "Order") to ensure the company abides by its data privacy and security obligations towards its users. The 2022 Order was not the first time Twitter had entered into a consent decree with the FTC; a previous investigation into Twitter had found serious security lapses and resulted in a 2011 Order.¹ When a firm has a history of repeat offenses, the FTC takes particular care to ensure compliance with its orders.

In early December 2022, media reports indicated Twitter had granted certain third-party individuals broad access to the company's systems, communications, and other information. For example, one individual tweeted on December 8, 2022, "Our team was given extensive, unfiltered access to Twitter's internal communications and systems."² Around the same time, another individual tweeted that "the authors have broad and expanding access to Twitter's files."³ Moreover, that same individual was reportedly given access to Twitter's employee systems, added to its Slack channel(s), and given a company laptop.⁴

¹ <https://www.ftc.gov/news-events/news/press-releases/2011/03/ftc-accepts-final-settlement-twitter-failure-safeguard-personal-information>

² <https://mobile.twitter.com/AbigailShrier/status/1601010924726284288>

³ <https://twitter.com/bariweiss/status/1601026062887972864>

⁴ <https://www.businessinsider.com/elon-musk-twitter-bari-weiss-cousins-confidants-2022-12>

Such statements triggered legal scrutiny because their breadth indicated that Twitter may have disclosed consumers' personal information—such as direct messages, protected Tweets, or information revealing real names or telephone numbers associated with a particular Twitter handle—in violation of the FTC's order and undermining user privacy. Compliance staff, therefore, sought information from Twitter about this development. Seeking information from a company as part of an order compliance investigation is a routine part of the FTC's work.

Here, for example, the Order prohibits Twitter from misrepresenting its privacy and security measures for preventing unauthorized access to information from or about individual consumers, and the Order further prohibits Twitter from misrepresenting the extent to which it makes such information accessible to any third parties.⁵ The Order also requires that Twitter have a comprehensive privacy and information security program with safeguards that include, at a minimum, data access policies and controls for: (a) all databases storing consumer information; (b) all networks, systems, and software that provide access to Twitter users' accounts; and (c) all networks, systems, and software containing information that enables or facilitates access to Twitter's internal network and systems.⁶

On their face, the individuals' public statements seemed to contradict what Twitter had previously told FTC compliance staff about its access policies and controls. Compliance staff therefore asked Twitter to describe the nature of any access it had granted to these third-party individuals and the circumstances in which such access had been permitted. They also asked Twitter to explain what measures, if any, it had taken to ensure these third parties did not gain unauthorized access to consumer information.

If Twitter had any confusion about whether the FTC's question sought information that extended beyond its data protection practices, it could have undertaken the routine step of calling FTC staff, and staff would have clarified the question. Twitter did not reach out to clarify any confusion; by contrast, Twitter correctly interpreted the question as limited to protections on consumer information, and FTC staff demonstrated the same reasonable understanding by accepting the appropriately limited answer.

Through the company's responses and depositions of former Twitter employees, FTC staff learned that the access provided to the third-party individuals turned out to be more limited than the individuals' tweets and other public reporting had indicated. The deposition testimony revealed that in early December 2022, Elon Musk had reportedly directed staff to grant an outside third-party individual "full access to everything at Twitter. . . . No limits at all."⁷ Consistent with Musk's direction, the individual was initially assigned a company laptop and internal account, with the intent that the third-party individual be given "elevated privileges" beyond what an average company employee might have.

However, based on a concern that such an arrangement would risk exposing nonpublic user information in potential violation of the FTC's Order, longtime information security employees at Twitter intervened and implemented safeguards to mitigate the risks. Ultimately the third-party individuals did not receive direct access to Twitter's systems, but instead worked with other company employees who accessed the systems on the individuals' behalf.

The FTC's investigation confirmed that staff was right to be concerned, given that Twitter's new CEO had directed employees to take actions that would have violated the FTC's Order. Once staff learned that the FTC's Order had worked to ensure that Twitter employees took appropriate measures to protect

⁵ See 2022 FTC Order I.A. & I.E.

⁶ See 2022 FTC Order V.E.7.

⁷ See F. Siddiqui, *Twitter Brings Elon Musk's Genius Reputation Crashing Down to Earth*, WASH. POST (Dec. 24, 2022), <https://perma.cc/7HLF-ELH9>.

consumers' private information, compliance staff made no further inquiries to Twitter or anyone else concerning this issue.

You also queried why the FTC was looking into personnel decisions made at Twitter. According to X Corporation (Twitter), in the fall of 2022, the company undertook a rapid series of terminations, layoffs, or other reductions in its workforce.⁸ Numerous employees also resigned during this time.⁹ These workforce reductions significantly impacted the Twitter teams charged with protecting user data. Key data privacy and security executives were gone, including the Chief Privacy Officer, the Chief Information Officer, and the Chief Compliance Officer. Simply put, there was no one left at the company responsible for interpreting and modifying data policies and practices to ensure Twitter was complying with the FTC's Order to safeguard Americans' personal data.

FTC staff efforts to ensure Twitter was in compliance with the Order were appropriate and necessary, especially given Twitter's history of privacy and security lapses and the fact that it had previously violated the 2011 FTC Order. During staff's evaluation of the workforce reductions, one of the company's recently departed lead privacy and security experts testified that Twitter Blue was being implemented too quickly so that the proper "security and privacy review was not conducted in accordance with the company's process for software development." Another expert testified that he had concerns about Mr. Musk's "commitment to overall security and privacy of the organization."¹⁰ Twitter, meanwhile, filed a motion seeking to eliminate the FTC Order that protected the privacy and security of Americans' data. Fortunately for Twitter's millions of users, that effort failed in court. The public interest is served by Twitter continuing to abide by its legal commitments under the Order, which include Twitter's agreement not to lie to consumers, the requirement to maintain a comprehensive program to protect consumers' information, and the requirement to offer enhanced account security features in a non-deceptive manner.

In the week before the FTC received the Committee's letter of February 14, 2024, FTC staff indicated that the Commission was working on providing the Committee with additional information. I hope this supplemental information answers some of your questions about the FTC's investigation of third-party access to Twitter user information and its review of the many terminations, layoffs, and resignations at Twitter. In addition, the Commission will be making a production of documents along with this letter.

Sincerely,



Lina M. Khan
Chair
Federal Trade Commission

cc: The Honorable Jerrold Nadler
Ranking Member
House Committee on the Judiciary

⁸ See Def. Ex. 5 filing in *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. May 25, 2022). See generally, Opposition to X Corp's Motion for Protective Order & Relief from Consent Order, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (Sept. 11, 2023) (previously provided to House Judiciary in September 2023).

⁹ *Id.*

¹⁰ *Id.*