



February 7, 2023

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

Dear Chair Khan,

I write to urge the Federal Trade Commission (FTC) to investigate new whistleblower allegations that Twitter has disregarded the privacy and security of its users and failed to abide by the terms of its consent decree with the Commission.

According to recent whistleblower disclosures, Twitter has failed to address serious deficiencies in its own privacy and security controls despite its legal obligations to do so under an FTC consent decree.¹ In one example documented by the new whistleblower, Twitter has continued to neglect internal vulnerabilities that allow any Twitter engineer to impersonate any Twitter user, a program once called “GodMode.” When pressed about the risk, according to the whistleblower, Twitter merely changed the name of the code rather than fixing the vulnerability. As the complaint notes, this incident illustrates Twitter management’s systemic failure to prioritize and address threats to the platform.

This new complaint serves as compelling and corroborating evidence of concerns raised in a prior whistleblower complaint. Previously, Peiter “Mudge” Zatkó, Twitter’s former Security Lead, alleged that the social media firm failed to address security vulnerabilities and mishandled personal data for more than a decade. According to the new whistleblower, those vulnerabilities remain knowingly unaddressed. I am particularly concerned about the implications of Twitter’s failures for U.S. national security. Both complaints demonstrate vulnerabilities in Twitter’s internal controls that would allow any of its thousands of employees to take over user accounts, raising acute concern about insider threats from foreign governments, especially in light of Mr. Zatkó’s disclosure noting examples of apparent espionage from China and India. Although “GodMode” may have changed in name, the risk of cybercriminals and malicious foreign actors

¹ “Ex-Twitter engineer tells FTC security violations persist after Musk.” Washington Post. <https://www.washingtonpost.com/technology/2023/01/24/whistleblower-twtter-ftc-settlement/>

abusing Twitter’s vulnerabilities—one of the risks that gave rise to the FTC’s May 2022 complaint against the platform—appears to remain high.

Furthermore, information provided by the whistleblower raises additional concerns that Twitter may be continuing to mishandle and misrepresent its use and retention of private data, including failing to delete information and misusing data collected from consumers. As Mr. Zatkan’s complaint previously described, Twitter appears to suffer from “ignorance and misuse of vast internal data sets,” which resulted in the failure to delete data upon request and the misuse of personal and security information for marketing purposes. The new whistleblower complaint suggests this misuse continues, adding that GodMode allows Twitter engineers to ‘undelete’ previously deleted tweets. Whether Twitter is properly handling requests to delete account data, such as tweets and direct messages, is especially significant to those individuals that have left the platform in recent months over concerns about security and the business practices of its new owner.

Most significantly and alarmingly, the new complaint describes conduct that occurred after Twitter agreed to implement stricter security controls pursuant to the May 2022 consent decree and after Elon Musk acquired the company in October 2022. The complaint goes beyond the timeframe covered by Mr. Zatkan’s disclosure — indeed, as much as a year after it, including details on neglect reported to continue after departures by key staff responsible for compliance with the consent decree and through today. Moreover, the complaint suggests that the “GodMode” vulnerability is merely “one more example” of how “Twitter’s public statements to users and investors were false and/or misleading.” Despite assurances to the public and Congress from Twitter about cleaning up its act, the platform has apparently continued to ignore not only threats to user safety and national security, but also its legal obligations under the consent decree. These continuing whistleblower claims suggest that additional violations and vulnerabilities may yet be uncovered.

I urge the Commission to vigorously investigate all allegations of Twitter’s consent decree violations, including the information provided by Mr. Zatkan and the new whistleblower. The FTC has a responsibility to bring enforcement actions—whether for any breach of Twitter’s consent decree or for other violations of our consumer protection laws—including seeking liability for individual Twitter executives, where appropriate.

Thank you for your attention to this important matter.

Sincerely,



Richard Blumenthal
United States Senate