

Twitter's former security chief says company lied about bots and safety

Twitter has hidden negligent security practices, misled federal regulators about its safety, and failed to properly estimate the number of bots on its platform, according to testimony from the company's former head of security, the legendary hacker-turned-cybersecurity-expert Peiter "Mudge" Zatko. The explosive allegations could have huge consequences, including federal fines and the potential unraveling of Tesla CEO Elon Musk's bid to buy Twitter.

Zatko was fired by Twitter in January and claims that this was retaliation for his refusal to stay quiet about the company's vulnerabilities. Last month, he filed a complaint with the Securities and Exchange Commission (SEC) that accuses Twitter of deceiving shareholders and violating an agreement it made with the Federal Trade Commission (FTC) to uphold certain security standards. His complaints, totaling more than 200 pages, were obtained by CNN and *The Washington Post* and published in redacted form this morning.

In an interview with CNN, Zatko said he joined Twitter in 2020 at the bequest of then-CEO Jack Dorsey, right after the company was hit by a massive hack in which accounts belonging to figures like Barack Obama, Bill Gates, and Kanye West were compromised. Zatko says he joined Twitter because he believes the platform is a "critical resource" for the world but became disillusioned by the refusal of CEO Parag Agrawal to tackle the company's many security failings.

"This would never be my first step, but I believe I am still

fulfilling my obligation to Jack and to users of the platform,” Zatkó told *The Washington Post* regarding his decision to become a whistleblower. “I want to finish the job Jack brought me in for, which is to improve the place.”

Zatkó’s disclosures to the SEC contain many damning reports and accusations, but these are some of the most significant:

- **Indiscriminate access.** A significant part of Twitter’s vulnerability is that too many employees have access to critical systems, claims Zatkó in his complaint. It states that around half of Twitter’s 7,000 or so full-time employees have access to users’ sensitive personal data (like phone numbers) and internal software (to alter how the service works) and that this access is not closely monitored. He also alleges that thousands of laptops contain complete copies of Twitter’s source code.
- **Misleading the FTC.** In 2010, Twitter settled charges with the FTC that it failed to protect consumers’ personal information – a significant and early example of government regulators reining in Big Tech. Zatkó’s complaint claims Twitter has repeatedly made “false and misleading statements” to users and the FTC, violating this agreement.
- **Ignoring bots.** Twitter has repeatedly claimed that less than 5 percent of its monthly daily active users are bots, fake accounts, or spam. Zatkó’s complaint says Twitter’s method of measuring this figure is misleading and that executives are incentivized (with bonuses of up to \$10 million) to boost user counts rather than remove spam bots.
- **Government agents.** Twitter is a key tool for sharing news and organizing protests, making it a ripe target for governments looking to crack down on dissent. Zatkó’s complaint states that he believes the Indian government forced Twitter to hire a government agent,

who then had “access to vast amounts of Twitter sensitive data.”

- **Failure to delete.** The complaint states that Twitter has, in the past, failed to delete users’ data when requested because such records are spread too widely among internal systems to be properly tracked. A current employee told *The Washington Post* that the company just completed a project, known as Project Eraser, to ensure proper deletion of user data.

In response to Zatko’s complaint, Twitter has accused its former chief of security of sensationalizing and selectively presenting information. A spokesperson told CNN:

“Mr. Zatko was fired from his senior executive role at Twitter for poor performance and ineffective leadership over six months ago. While we haven’t had access to the specific allegations being referenced, what we’ve seen so far is a narrative about our privacy and data security practices that is riddled with inconsistencies and inaccuracies, and lacks important context. Mr. Zatko’s allegations and opportunistic timing appear designed to capture attention and inflict harm on Twitter, its customers and its shareholders. Security and privacy have long been company-wide priorities at Twitter and we still have a lot of work ahead of us.”

Zatko’s allegations are explosive and will have a significant effect on the company. The FTC is currently reviewing the complaint, according to sources cited by *The Washington Post*, and would likely levy significant fines against Twitter if Zatko’s accusations are proven to be correct.

The complaint will also affect the ongoing struggle between Musk and Twitter. Musk is currently trying to extricate himself from a \$44 billion agreement to buy the company, justifying the decision with an accusation that Twitter is lying about the true number of bot and spam accounts on the

platform. "We have already issued a subpoena for Mr. Zatko," Alex Spiro, a lawyer representing Musk, said in a statement, "and we found his exit and that of other key employees curious in light of what we have been finding."

Although it's not clear if Zatko's complaint affects Musk's legal argument, it will certainly strengthen the public perception of his case, which is based on the accusation that Twitter is undercounting its bots.

Update August 23rd, 9:35AM ET: Added comment from Elon Musk's lawyer.

<https://www.theverge.com/2022/8/23/23317857/twitter-whistleblower-zatko-security-spam-safety>