KATZ BANKS KUMIN

WHISTLEBLOWER AID

Written Statement of Peiter ("Mudge") Zatko
United States Senate Judiciary Committee
September 13, 2022

Chairman Durbin, Ranking Member Grassley, and Members of the Committee. At your request, I appear before you today to answer questions about information I submitted in written disclosures about cybersecurity concerns I raised and observed while working at Twitter.

My name is Peiter Zatko, but I am often still called by "Mudge," my online handle. From November 2020 until January 2022, I was Twitter's "Security Lead," a senior executive role in which I was responsible for Information Security, Privacy Engineering, Physical Security, Information Technology, and Twitter Services, the company's global support and enforcement division.

For 30 years, my mission has been to make the world better by making it more secure. As a cybersecurity expert with over a decade of senior leadership experience, I identify and balance cybersecurity vulnerabilities with business goals. The cybersecurity vulnerabilities I deal with expose individuals, organizations, and the United States to risk and attacks that cause physical, financial, and emotional harm.

I agreed to join Twitter because I believed it was a unique position in which my skills and experience could meaningfully improve the security of users, the United States, and the world. Twitter was and continues to be one of the world's most influential communications platforms. What happens on Twitter has an outsized effect on public discourse and our culture. I believed that improving the platform's security would benefit not only Twitter's millions of users, but also the people, communities, and institutions affected by the information exchanges and debates taking place on the platform.

To understand how I got here today, however, I think it is important you know about my past.

Since the 1990s, I have been a pioneer in the computer and information security field, including helping to found the responsible disclosure movement, which some people refer to as "ethical hacking." The responsible reporting of security problems aims to inform people and institutions about cybersecurity vulnerabilities and to show them how to strengthen security.

When a responsible practitioner finds a vulnerability that bad actors can exploit, the person first makes a quiet disclosure directly to the institution, giving the affected company or government the information and the opportunity needed to fix the vulnerability. If the vulnerable institution does not want to hear the truth or fix the problem, the person reporting the problem must determine if public disclosure of the unaddressed security vulnerability is necessary to protect the public. If the benefit of public disclosure outweighs the risk to the recalcitrant institution, then the responsible practitioner makes the public disclosure necessary to alert the public to the risk and to encourage the institution to address the vulnerability.

I continue to follow this ethical disclosure philosophy and am here today because I believe that Twitter's unsafe handling of the data of its users and its inability or unwillingness to truthfully represent issues to its board of directors and regulators have created real risk to tens of millions of Americans, the American democratic process, and America's national security. Further, I believe that Twitter's willingness to purposely mislead regulatory agencies violates Twitter's legal obligations and cannot be ethically condoned.

Given the potential harm to the public of Twitter's unwillingness to address problems I reported and Twitter's continued efforts to cover up those problems, I determined lawful disclosure was necessary despite the personal and professional risk to me and my family of becoming a whistleblower.

This is not the first time I have had to deal with critical cybersecurity vulnerabilities. I have advised a sitting president, administrations of both parties, Congress, and the intelligence community on these issues. In 2010, I accepted an appointed position in charge of running Cyber Programs for the Department of Defense and Intelligence Communities at DARPA; for my service, I became a decorated civilian after being awarded the medal for exceptional public service (the highest medal able to be bestowed upon a non-career civilian by the Office of the Secretary of Defense). I then returned to the private sector and worked in senior leadership positions for companies like Motorola, Google, and Stripe, where I continued to help those companies focus on protecting companies and users from security risks.

I joined Twitter after it was infamously hacked by a group of teenagers, who launched what was then the largest hack of a social media platform in history. They took over the accounts of high-profile Twitter users as part of a crypto-currency scam. Afterward, Twitter's then-Chief Executive Officer, Jack Dorsey, reached out to me because of my unique breadth of experience in security, asking if I would join the company to assess the state of its security and make fundamental changes.

Experience, however, has taught me that making big changes to improve security is hard. And hard changes draw intense opposition from people who profit from the status quo. It was clear to me, however, that Jack Dorsey was committed to change, so I accepted the challenge. In doing so, I made a personal commitment to Twitter, the greater public, and to myself that I would do my best to drive the changes that Twitter – and its users and our democracy – desperately needed.

I have lived by that commitment.

Upon joining Twitter, I discovered that the Company had 10 years of overdue critical security issues, and it was not making meaningful progress on them. This was a ticking bomb of security vulnerabilities. Staying true to my ethical disclosure philosophy, I repeatedly disclosed those security failures to the highest levels of the Company. It was only after my reports went unheeded that I submitted my disclosures to government agencies and regulators.

In those disclosures, I detail how the Company leadership misled its Board of Directors, regulators, and the public. Twitter's security failures threaten national security, compromise the privacy and security of users, and at times threaten the very continued existence of the Company. I also detail that despite these grave threats, Twitter leadership has refused to make the tough but necessary changes to create a secure platform. Instead, Twitter leadership has repeatedly covered up its security failures by duping regulators and lying to users and investors.

I did not make my whistleblower disclosures out of spite or to harm Twitter. Far from that. I continue to believe in the mission of Twitter and root for its success. But that success can only happen if the privacy and security of Twitter's users and the public are protected. Many of the engineers and employees within Twitter have been repeatedly calling for this, but their calls are not being headed by the executive team.

It became clear by Twitter's actions that the only path to achieve that outcome was through lawful disclosure. My genuine hope is that my disclosures help Twitter finally address its security failures and encourage the Company to listen to its engineers and employees who have long reported the same issues I have disclosed.

I stand by the statements I made in my disclosures and am here to answer any questions you have about them.

Thank you.