— SENSITIVE & CONFIDENTIAL WHISTLEBLOWER DISCLOSURE —

July 6, 2022

Honorable Mark Warner, Chair
Honorable Marco Rubio, Vice Chair
U.S. Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, D.C. 20510

Jay Bratt, Chief
Counterintelligence and Export Controls Section
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W., Ste. 7700
Washington, D.C. 20530-0001
Via FedEx or Hand Delivery

Re: Protected Disclosures of Suspected Penetration of Twitter, Inc. by Multiple Foreign Intelligence Agencies, and Other Threats to U.S. National Security

Dear Senator Warner, Senator Rubio and Mr. Bratt:

1. We respectfully request that this disclosure remain confidential for reasons of personal privacy, threats to health and safety, and U.S. national security.

2. We are lawyers representing **Peiter "Mudge" Zatko**, who was employed as "Security Lead", a member of the executive team responsible for Information Security, Privacy, Physical Security, Information Technology, and Twitter Service (the company's internal name for the division responsible for global content moderation enforcement), at **Twitter, Inc.** from November 16, 2020, until the morning of January 19, 2022, when CEO Parag Agrawal terminated Mr. Zatko after Mr. Zatko alleged fraud by Mr. Agrawal.

3. Before joining Twitter, Mr. Zatko held senior positions at Google and Stripe, and within the **Department of Defense**,[1] where he was authorized to access **Top Secret / Special Compartmented Information** for work on programs at the bleeding edge of full-spectrum computer network operations. The Office of the Secretary of Defense bestowed upon Mr. Zatko the **Exceptional Public Service Award**, the highest honor available to civilian, non-career officials. The value of Mr. Zatko's work for the United States has also been formally recognized by the CIA, White House, and U.S. Army.

4. Mr. Zatko decided to proceed with these disclosures quite reluctantly.[2] Under separate cover, Mr. Zatko is simultaneously making protected, lawful disclosures[3] to the U.S. Securities and Exchange Commission (SEC), U.S. Federal Trade Commission (FTC), and Department of Justice (DOJ) of substantial evidence showing that Twitter, Inc., CEO Parag Agrawal, as well as particular senior executives and members of its Board of Directors, since 2011 and on an ongoing basis, have engaged in:

    a. Extensive, repeated, uninterrupted violations of the Federal Trade Commission Act by making false and misleading statements to users and the FTC about, *inter alia*, the Twitter platform's security, privacy, and integrity;

    b. Violations of various securities laws including auditing and financial control provisions;

    c. Fraudulent and material misrepresentations in communications with the Board of Directors and investors, constituting securities law violations;

---

[1] See https://en.wikipedia.org/wiki/Peiter_Zatko. Former Twitter CEO Jack Dorsey cited this track record of speaking truth to power as a primary reason for recruiting Mr. Zatko.

[2] Mr. Zatko helped create the modern information security community of ethical security disclosures. While criminals break and steal, independent security researchers (also known as "ethical hackers") use their skills to inform people about specific vulnerabilities, strengthen security and advance human rights and democracy. When ethical hackers find a vulnerability that bad actors can exploit, they first make a quiet "responsible disclosure" so that the affected company or government can fix it. But sometimes, the vulnerable institution doesn't want to hear the truth, or fix the problem. In those cases, ethical researchers are forced to weigh the risks of wider disclosure: Exposing vulnerabilities tips off bad actors, but it also allows users of a service to make more informed decisions, and can push the service to improve. Mr. Zatko made a personal commitment to Mr. Dorsey, the Twitter Board, the greater public, and to himself, that he would do his best to help fix Twitter. Mr. Zatko spent about 14 months pushing improvements from the inside, and was terminated for his efforts. With a heavy heart, Mr. Zatko has concluded that these lawful disclosures are his ethical obligation. Mr. Zatko has tried his best to avoid disclosing unnecessary technical or sensitive information.

[3] The separate SEC / FTC disclosure is included as an exhibit to this document.

5. But this instant disclosure has a different focus: Twitter's negligence and even complicity with respect to efforts by **foreign governments to infiltrate, control, exploit, surveil and/or censor** the company's users, platform, staff, and operations. This disclosure includes information and an exhibit not contained in the SEC / FTC disclosure.

6. **No Privileged Contents:** Upon information and belief, no attorney-client privileged material, information or documents are included here. None of the information or documents provided here were received from a lawyer, part of a communication with a lawyer, or obtained for the purpose of seeking legal advice.

II. Twitter's Deficiencies Threaten Users and Global Security

7. Except for a few jurisdictions in which Twitter is blocked or censored at mass scale, [4] Twitter is available in most of the countries on earth. Dozens of the countries in which Twitter operates are unfriendly to democracy, as determined by Freedom House.[5] Twitter hold the sensitive data (not just content, but information that can reveal geo-locations) of hundreds of millions of users around the world, but its efforts to protect that data are drastically deficient.

8. **Twitter is a soft target:** To cite merely one pervasive problem, **over 50% of Twitter staff are engineers—about 4000 people around the world—and all engineers have direct access to Twitter's production environment with live user data and access to Twitter's full source tree**. This is highly unusual, and highly insecure. Other large tech companies have controlled environments for testing new code; if engineers are based in hostile countries their access to live user data should be strictly limited.[6] In addition to the significant exposure this presents to Twitter's systems and data in their production environment, Twitter was made aware by the US Government that portions of the source code at the company were controlled items as determined by the Export Administration Regulations by the Department of Commerce. Twitter was aware that the company was required by law to deny access to particular foreign national employees, but was unable to implement that

[4] "Censorship of Twitter - Wikipedia." https://en.wikipedia.org/wiki/Censorship_of_Twitter.
[5] "Freedom in the World." https://freedomhouse.org/report/freedom-world.
[6] Several companies refuse to place engineers in specific countries and/or maintain the ability to cut off access to entire offices. At Twitter all employees have excessive access to information that they shouldn't and it is presently impossible to cut engineers off from production system access.

legal requirement because of system architecture flaws. The significance of types of access and lack of controls to prevent inappropriate access from both internal and external entities are described further in the SEC / FTC disclosure.

9. Historically Twitter had been caught without any language translation capabilities prior to significant world events leaving them far behind their peers, unable to perform basic moderation, support, and analysis of platform manipulation by foreign entities. Twitter was caught unprepared for basic translation and language abilities to protect the platform and users from abuse and manipulations repeatedly. Twitter lacked language support and capabilities to support the forcible displacement and ethnic violence in Tigray, Ethiopia (Ahmaric and Oromo) Q1, 2021. Twitter lacked Burmese language ability when the military coup in February 2021 occurred in Myanmar. The company lacked language support and capabilities to support the platform during the US withdrawal from Afghanistan (Pashto and Dari). All of these shortcomings meant Twitter was largely blind to what purposes, and how, its platform was being used during these geopolitical crises.

10. **Perverse incentives to grow total users:** Twitter executives have personal financial incentives ("Value Creation Awards" exceeding $10 million each) for achieving aggressive global growth targets for "mDAU" (monetizable daily active users). Mr. Zatko believes that they are willing to look the other way and/or avoid confronting many of the problems identified in this disclosure and in the separate SEC/ FTC disclosure because they were not rewarded for advancing security, privacy or platform integrity (e.g. stopping disinformation and election meddling). To the contrary, such objectives detracted from growth.

11. These dynamics led Twitter to pursue aggressive expansion into new markets, including non-democratic states where governments were likely to impose problematic conditions in exchange for giving the company access to their citizens. Chasing growth, leadership refused to address a critical problem — the company's technical inability to deter, identify, or remediate activities to protect user data from the adversarial governments of the territories into which the company was expanding. Twitter is simply not capable of expanding into such undemocratic markets while protecting its users' data, and hence safety, from those governments. Across every dimension, monetary bonus incentives for executives rewarded short-term growth at the expense of longer-term safety, privacy and integrity.

12. **Squeezing Local Staff:** Countries where Twitter had a physical presence, including actual full time employees (FTEs), and particularly where Twitter had official offices, represented heightened risk to Twitter and the Twitter platform. In addition to the risk exposed by Twitter's fundamental lack of information security and privacy control, described in other disclosures, there was the physical safety of the employees to consider. The threat of harm to Twitter employees was sufficient to cause Twitter to seriously consider complying with foreign government requests that Twitter would otherwise fundamentally oppose.

13. **Foreign Agents on Company Payroll:** Even active foreign intelligence threats like information operations on the platform, and foreign agents on Twitter's payroll, were left unaddressed because of their expected negative impact on short-term mDAU growth. During his time as Security Lead, Mr. Zatko determined with high confidence that foreign governments continued to target Twitter and had successfully placed multiple intelligence agents on Twitter's payroll. Accordingly, it was highly likely internal Twitter systems were compromised by state actors. Even though this problem had happened before,[7] the Twitter leadership team resisted viewing this as a serious concern. Impediments to fixing the issue included a lack of detection or enforcement systems.[8] The lack of visibility to monitor internal activities, significant out of date software, misconfigured employee computers, and lack of access control and data protection are described in detail in the enclosed FTC / SEC disclosure.

14. **India's intelligence agency**, known as the **Research and Analysis Wing (R&AW)**, targeted Twitter physically and electronically[9], and forced Twitter to hire two

[7] "Twitter Insiders Allegedly Spied for Saudi Arabia - WIRED." 6 Nov. 2019, https://www.wired.com/story/twitter-insiders-saudi-arabia-spy/.

[8] For example, around August 13th 2021 it was internally revealed that between 1.5 and 3 *thousand* failed login attempts per day were occuring in Twitter's production environment. Additionally, as reported to the Board of Directors in 2021, centralized logging was not mature and only covered <~20% of systems and services. This lack of basic security hygiene was not relegated to only Twitter's data centers. Approximately ⅓ of the employee laptops were reporting they had disabled software updates. Employee computers were also reporting that they had disabled disk encryption, turned off their firewalls, were configured to allow remote access, and other significant lack of basic protections. As was reported to the Board of Directors in the 2021 Q4 Privacy briefing, because of fundamental and systemic problems with security and access control, all employees of Twitter have access to significantly more data than they need to perform their jobs.

[9] One item was a "raid" of Twitter offices in the middle of the night during pandemic lockdown. This does not support the India Special Cell police claim that they were there to talk to employees about a Tweet. The Special Cell also brought "media teams" with equipment for this visit to Twitter offices in the middle of the night during the pandemic lockdown expecting to find people at the office that they could interrogate.

particular agents of the Indian government. The Indian government also ran harassment campaigns against specific Twitter India employees,[10] including repeatedly requiring Twitter's India site lead to come to police stations, answer questions and surrender his electronic devices for significant periods of time during which the devices were believed likely to have been penetrated and/or imaged. Through these physical and online campaigns it is believed the Indian government was able to co-opt and manipulate at least one company employee to act as an agent of the Indian government. Another person, intending to fill a role required by the Indian government, was revealed as having a fabricated history not unlike those created for spies and intelligence agents.

15. An Indian Court, the police, and members of the **Ministry of Electronics and Information Technology (MEITY)** pushed the company to make these individuals Full Time Employees (FTEs), a status which would provide access to internal systems and documents. In one case, a custom system was spun up at significant effort to create a minimal-access environment that would allow them to perform their job, but not have the excessive access to information all other employees at the company were granted. This particular employee immediately requested copies of any legal documents and strategies Twitter was preparing regarding the Indian Court—an anomalous, out-of-role request according to the employee's manager and executive team members, that strengthened suspicions they were a government agent.

16. Twitter has hundreds of employees in India, all of whom have significant access to data far beyond what they need for their jobs. About 80 of those were engineers with full access to Twitter's source tree and default access to connect to systems and access data in Twitter's production environments. But design flaws in Twitter's system architecture made it impossible to reduce sensitive system access, or

"Police in India raid Twitter offices in probe of tweets with ... - The Verge." 24 May. 2021, https://www.theverge.com/2021/5/24/22451271/police-india-raid-twitter-tweets-government-manipulated-media. The use of India Special Cell police is a tactic that is rumored to be employed by R&AW in their targeting and instrumentation efforts.

[10] These included the public media in India targeting Twitter India individuals and visits to their houses and their relatives houses by the police. One individual suffered multiple police summons. Some of these included confiscation, and return, of his phone. Twitter personal cell phones are permitted access to large amounts of sensitive Twitter internal information and were also used to support authentication to other Twitter systems. Ultimately this person fled to the United States. Ultimately, after being targeted repeatedly by India's police, Courts, and newspapers, Twitter brought him to the US for an extended period for safety. Having agreed to follow very specific instructions to preserve the status of his cell phone, to allow for forensic analysis, he decided to completely erase and reset the device right before handing it over to Twitter Security. This removed any ability to perform appropriate forensic analysis.

identify or monitor for insider threat activity. Further, the harassment and threat of jail time to Indian citizens working for Twitter India, for the company not censoring certain tweets or handing over information on protesters' accounts carried weight.

17. Mr. Zatko repeatedly requested that the topic of whether to leave India and serve those users from outside the country, or invest in fixing the fundamental deficiencies be brought up for an executive decision. Even though several executives including the CEO Jack Dorsey expressed some support for leaving the market due to the physical and geopolitical risks, the topic was repeatedly tabled and never addressed. In one conversation with another executive Mr. Zatko explained the severity of the insider threat problem and why Twitter needed to consider leaving the environment. The executive replied along the lines of "if we already have one insider threat from the Indian government why does it matter if we have more?" There was too much revenue potential in India so Twitter should just accept the compromise, was a prevailing attitude for several executives.

18. **Selective disclosure of government backed influence operations.** Based upon information and belief, Twitter has a policy to publicly disclose attempts by state-linked entities to manipulate Twitter and its users[11]. As such, anytime they become aware of a governmental operation within their system, they should report on it publicly. Contrary to Twitter's own transparency principles they had been aware of an information operation being run by a branch of the Indian Army,[12] yet were refusing to include this information in their information operations transparency disclosures. (While Twitter was refusing to disclose information about Indian backed Information Operations, they released information about operations from other countries including India's rival Pakistan.)

19. Twitter staff approached Mr. Zatko confidentially, and told him that the direction to withhold disclosure of the Indian operations had been going on for almost a year.[13] (The staff hoped Mr. Zatko, in his senior executive role, could intervene to fix this.) Discussing the issue in both executive team meetings and in personal conversations it was revealed that the decision to not report Indian operations was

[11] "Information Operations - Twitter Transparency Center." https://transparency.twitter.com/en/reports/information-operations.html.
[12] The Indian Army branch believed responsible for repeatedly attempting and running information operations was Corps XV, also referred to as the Chinar Corps. https://en.wikipedia.org/wiki/XV_Corps_(India)
[13] According to personal notes on, or about, August 2nd, 2021, Site Integrity, the team responsible for disclosure of information operations told this to Mr. Zatko.

driven by a desire to curry favor with the Bharatiya Janata Party (BJP) and India's courts. Offending the BJP and India's Courts could be detrimental to Twitter employees in the country and user growth on the service. If India took action against the company it could ultimately negatively impact user growth numbers.

20. **Additional / Separate Foreign Agent:** Based upon information and belief, shortly before Mr. Zatko was terminated, Twitter was made aware of **at least one additional employee who was identified as a foreign agent**[14] working on behalf of another foreign intelligence agency. Given the global importance and value of the platform, broad system and data access, and unlikeliness of being discovered, foreign intelligence services would not be doing their job if they were not attempting to place agents, or recruit existing employees, inside Twitter. It is very likely that there are more foreign agents than those being disclosed that are operating undetected and relatively unrestricted within Twitter.

21. **Threats to Democracy:** Over the course of 2021, Mr. Zatko became aware of multiple episodes suggesting that Twitter was complicit in threats to democratic governance. In addition to India's efforts described above, several other countries were demanding Twitter open regional offices with actual Twitter employees in residence. **Turkey, Russia, and Nigeria** were three countries pressuring Twitter to stand up local offices with full time employees.

22. **Turkey.** Mr. Zatko provided a briefing on Turkey and the capabilities and risks presented to Twitter by Turkey's National Intelligence Organization (TNIO) and strongly urged the executive team to not open an office. Even with this information it seemed as though Twitter was looking at opening an office in Turkey. Mr. Zatko later learned that Twitter measured a meaningful amount of monetizable users[15] in Turkey.

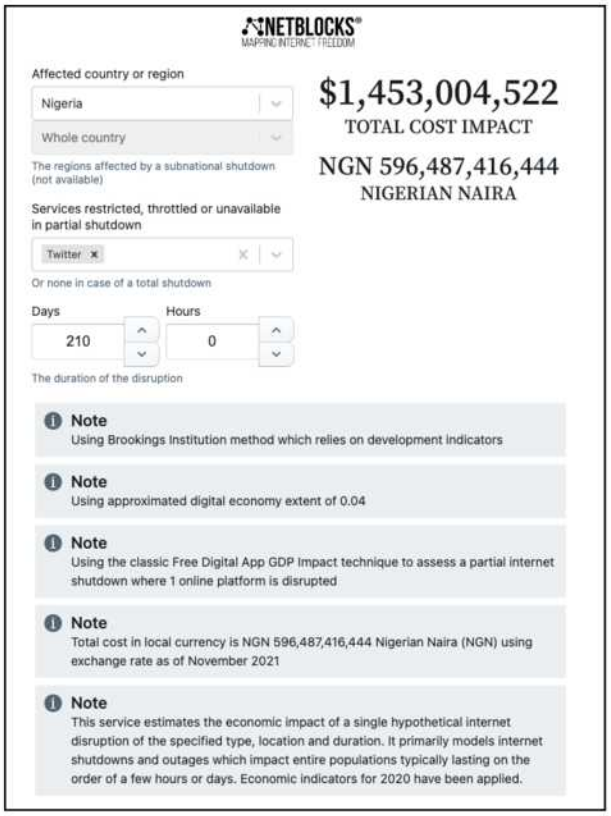
23. **Nigeria:** Nigeria was perceived as important for growing Twitter's user base. Immediately upon joining Twitter in late 2020, Mr. Zatko lobbied with others (successfully) to not open physical offices in Nigeria but rather to serve the Nigeria market with offices based in nearby Ghana. The Nigerian government was viewed as unstable and unpredictable, and banned Twitter on June 5, 2021.

[14] The existence of another employee identified as a foreign agent had been reported from an external source to the Twitter CorpSec team. CorpSec is a team within Mr. Zatko's organization and this bit of information was reported up to him.
[15] Twitter stock value was largely dependent upon measurements of "monetizeable" users, referred to as mDAU.

24. After that, the Nigerian government falsely, and repeatedly, reported in the Nigerian press, which was picked up worldwide, that it was in talks with Twitter leadership.[16] For months, there were numerous false reports put forward by the Nigerian government describing non-existent meetings further describing various progress and setbacks being made in negotiations with Twitter. The truth was that the Nigerian government refused any and all meetings with Twitter to discuss the topic for months. Instead of meeting with Twitter the Nigerian government chose to repeatedly publish media articles saying they are in the midst of fabricated negotiations with Twitter and are almost at the point of agreement to end the ban. Nigeria even announced that Twitter had agreed in the negotiations to open a Nigeria office.[17] Twitter's failure to correct the public lies purporting to characterize non-existent negotiations enabled Nigeria to continue pushing their false narratives.

25. The false information, to which Twitter was now a party by not addressing, accomplished two things: 1) international human rights organizations were more willing to refrain from pushing as hard as they had initial censorship of the Nigerian people, and 2) Twitter shareholders were permitted to believe that the company would soon start to again be monetizing approximately 36.9 Million Twitter users in Nigeria.[18] The NetBlocks Cost Of Shutdown Tool, using methods from The Brookings Institute estimates a total monetary loss to the Nigerian economy due to the support of this public lie at approximately $1.4 billion dollars:[19]

[16] "What Buhari said about Twitter ban, Nnamdi Kanu, Igboho ...." 1 Oct. 2021, https://www.premiumtimesng.com/news/top-news/487593-what-buhari-said-about-twitter-ban-nnamdi-kanu-igboho-insecurity-others-full-text.html. Accessed 28 Apr. 2022.
[17] More details included in Exhibit 39.
[18] 39.6M users were mostly upwardly mobile economically and politically, with 20% using the platform for advertisement, and 18% using Twitter to look for employment according to a Twitter contractor who sent in information about the Nigeria situation at the time.
[19] This value is derived from the NetBlocks Cost of Shutdown Tool using 210 days and the shutdown of Twitter in Nigeria as input. From their website "The NetBlocks Cost of Shutdown Tool (COST) estimates the economic impact of an internet disruption, mobile data outage or app restriction using indicators from the World Bank, ITU, Eurostat and U.S. Census." "Cost of Shutdown Tool - NetBlocks." https://netblocks.org/cost/.



26. On the Nigeria matter, Mr. Zatko sent repeated messages to senior executives including the new head of communications[20] from June through November 2021, requesting that Twitter correct the public record. Twitter's failure to do so misled investors and the international community on an important issue.

27. **Russia:** Russia was not viewed as important for user growth, and as such Twitter resisted the government's demands to place FTEs in Russia. But in or around September, 2021, a few months before then-CTO Parag Agrawal was promoted to CEO, in an in-person meeting in New York City Mr. Agrawal suggested to Mr. Zatko that Twitter should **consider ceding to the Russian Federation**'s censorship and surveillance demands. Although Mr. Agrawal's suggestion was never pursued or implemented, the fact that Twitter's current CEO even suggested Twitter become complicit with the Putin regime is cause for concern about Twitter's effects on U.S. national security. This was a strong departure from the message Mr. Dorsey had conveyed to Mr. Zatko. This interaction was notable because Mr. Zatko was already directing teams to prepare for possible Russian incursions into Ukraine.

[20] These were predominantly Signal.app messages from Mr. Zatko, based on personal notes.

28. **China:** Twitter executives opted to allow Twitter to become more dependent upon revenue coming from Chinese entities even though the Twitter service is blocked in China. After Chinese entities paid money to Twitter, there were concerns within Twitter that the information the Chinese entities could receive would allow them to identify and learn sensitive information about Chinese users who successfully circumvented the block, and other users around the world. Twitter executives knew that accepting Chinese money risked endangering users in China (where employing VPNs or other circumvention technologies to access the platform is prohibited) and elsewhere. Twitter executives understood this constituted a major ethical compromise. Mr. Zatko was told that Twitter was too dependent upon the revenue stream at this point to do anything other than attempt to increase it.

29. In none of these cases did Twitter act responsibly under the circumstances.

---

30. Our client would be willing to meet with investigators at your convenience. Please feel free to contact us using the information below.

31. Whistleblower Aid is a non-profit legal organization that helps workers report their concerns about violations of the law safely, lawfully, and responsibly. We respectfully request your assistance ensuring that our client never faces retaliation.

Sincerely,

Mark S. Zaid
Founder & Legal Partner

John N. Tye, attorney at law
Founder & Chief Disclosure Officer
[redacted]

[redacted]

Andrew P. Bakaj
Senior Counsel
[redacted]

Kyle Gardiner
Associate Counsel
[redacted]
Whistleblower Aid
[redacted]

Exhibits Enclosed:

1. SEC & FTC disclosure, filed separately as Exhibit A1

A1	SEC / FTC disclosure, filed separately (Link to come)
B1	Exhibit B1_20211001_Mudge Twitter Nigeria Notes_redacted
B2	Exhibit B2_202103xx_2021 Q3 or Q4 Risk Committee closed session meeting on foreign agent employee

B3	Exhibit B3_Mudge moleskine + phone notes Dec 2020 Feb 2022
B4	Exhibit B4_202112xx_Insider_Risk_December_2021
B5	Exhibit B5_2021XXXX_Snapshot of data center security system deficiencies_redacted
B6	https://drive.google.com/file/d/1_0hAm3WAKq3Osis4WJMjJsVFUHU2ld66/view?usp=sharing

END OF DISCLOSURE