

POMERANTZ LLP
Jennifer Pafiti (SBN 282790)
1100 Glendon Avenue, 15th Floor
Los Angeles, California 90024
Telephone: (310) 405-7190
jpafiti@pomlaw.com

*Counsel for Court-Appointed Lead Plaintiff
William Baker, Additional Plaintiffs
Mohammed Thaseen and Jill Sligay,
and Co-Lead Counsel for the Proposed Class*

[additional counsel on signature page]

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

WILLIAM BAKER, MOHAMMED
THASEEN, JILL SLIGAY, LENARD
ROQUE, and AMOLKUMAR
VAIDYA, Individually and on Behalf of
All Others Similarly Situated,

Plaintiffs,

v.

TWITTER, INC., JACK DORSEY,
NED SEGAL, PARAG AGRAWAL,
VIJAYA GADDE, and KAYVON
BEYKPOUR,

Defendants.

Case No. 2:22-cv-06525-MCS-E

AMENDED CLASS ACTION
COMPLAINT FOR VIOLATIONS
OF THE FEDERAL SECURITIES
LAWS

CLASS ACTION

JURY TRIAL DEMANDED

TABLE OF CONTENTS

I.	NATURE OF THE ACTION	6
II.	JURISDICTION AND VENUE	14
III.	PARTIES	15
A.	Plaintiffs	15
B.	Defendants	15
C.	Relevant Non-Parties.....	17
IV.	SUBSTANTIVE ALLEGATIONS	19
A.	Twitter’s Repeated Security and Privacy Incidents Lead to an FTC Consent Order.....	19
B.	In 2020, Twitter Experiences a Major Cybersecurity Incident.....	22
C.	In 2020, the FTC Takes Further Action Against Twitter.....	23
D.	Twitter Recruits Zatkan as Security/Integrity Lead.....	23
E.	Zatkan Becomes a Whistleblower.....	24
F.	Zatkan at Twitter	25
1.	February 2021 Executive Meeting.....	27
2.	Alethea report.....	34
3.	Zatkan Tells the Board Risk Committee Facts Showing that Twitter Is Not Complying with the FTC Consent Order	36
4.	Twitter Violates the FTC Consent Order by Using Customer Data for Purposes the User Had Not Consented to Even as It Is Negotiating A Fine For Doing the Exact Same Thing	38
5.	Failed Logins.....	39
6.	Log4j	40

1	7.	Insecure software	41
2	8.	Agrawal Fires Zatko for Blowing the Whistle.....	43
3	9.	February 2022 report.....	48
4	10.	Zatko Raises Critical Deficiencies, Only to Learn that Twitter	
5		Had Known of and Buried Them.....	50
6	G.	Defendants Make False Statements About mDAU.....	58
7			
8	1.	Almost a Third of Users Counted in mDAU Never Saw Any	
9		Ads	60
10	2.	Twitter Knowingly Mislabeled Spam Accounts and Bots	
11		Within mDAU	61
12	3.	Far More than 5% of mDAU and of Twitter’s User Base	
13		Consisted of Fake and Spam Accounts.....	64
14	4.	mDAU Was Not a Key Metric Inside Twitter, But Was Used to	
15		Cover Up Declining User Engagement	68
16	H.	A second whistleblower confirms Zatko’s claims	69
17	V.	DEFENDANTS’ MISSTATEMENTS	71
18	A.	Misstatements Implicating Compliance with the FTC Consent Order	73
19			
20	1.	Class Period Reports on Forms 10-K and 10-Q	74
21	2.	Statements in Presentations and Conferences.....	76
22	3.	Official Twitter Blog posts	83
23	4.	Agrawal interview with Wired magazine	89
24	B.	Misstatements Concerning mDAU	89
25			
26	1.	Class Period Reports on Forms 10-K and 10-Q	90
27	2.	Conference Calls and Presentations.....	93
28	3.	September 21, 2021 Tweet	94

1	4. Defendant Agrawal’s False and Misleading Tweets in May	
2	2022	96
3	C. Misstatements Implicating Twitter’s Use of Stolen Intellectual	
4	Property	96
5	VI. LOSS CAUSATION	99
6	VII. PRESUMPTION OF RELIANCE	104
7	VIII. INAPPLICABILITY OF STATUTORY SAFE HARBOR OR BESPEAKS	
8	CAUTION DOCTRINE	107
9	IX. CLASS ACTION ALLEGATIONS.....	108
10	X. COUNTS	110
11	COUNT I	110
12	(Violations of Section 10(b) of the Exchange Act, and Rule 10b-5	
13	Thereunder, Against Defendants)	110
14	COUNT II.....	112
15	(Violations of Section 20(a) of the Exchange Act Against the Individual	
16	Defendants)	112
17	XI. PRAYER FOR RELIEF	113
18	XII. JURY TRIAL DEMANDED.....	114
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

1 Court-appointed Lead Plaintiff William Baker (“Lead Plaintiff”) and additional
2 plaintiff(s) Mohammed Thaseen, Jill Sligay, Lenard Roque, and Amolkumar Vaidya
3 (“Additional Plaintiffs”, and with Lead Plaintiff, “Plaintiffs”), individually and on behalf
4 of all others similarly situated, by Plaintiffs’ undersigned counsel, hereby bring this
5 Amended Class Action Complaint (the “Complaint”) against Twitter, Inc. (“Twitter” or
6 the “Company”), Jack Dorsey, Ned Segal, Parag Agrawal, and Vijaya Gadde
7
8 (collectively, “Defendants”).
9

10 Plaintiffs’ claims are brought upon personal knowledge, as to Plaintiffs and
11 Plaintiffs’ own acts, and upon information and belief, as to all other matters, based on
12 the investigation conducted by and through Plaintiffs’ attorneys, which included, among
13 other things, a review and analysis of: (1) reports and documents filed by Twitter with
14 the U.S. Securities and Exchange Commission (“SEC”); (2) reports issued by securities
15 analysts concerning Twitter; (3) press releases, news articles, transcripts, and other
16 public statements issued by or about Twitter; (4) an investigation conducted by
17 Plaintiffs’ attorneys, including interviews with former employees of Twitter; (5)
18 confirmation of the truth of the allegations made by Twitter’s former Head of Security,
19 Peiter “Mudge” Zatko, in a whistleblower disclosure to the Federal government and in
20 testimony to a U.S. Senate committee; and (6) other publicly-available information
21 concerning Defendants. Plaintiffs’ investigation into the matters alleged herein is
22 continuing and many relevant facts are known only to, or are exclusively within the
23
24
25
26
27
28

1 custody and control of, Defendants. Plaintiffs believe that substantial additional
2 evidentiary support will exist for the allegations set forth herein after a reasonable
3 opportunity for discovery.
4

5 **I. NATURE OF THE ACTION¹**

6 1. This is a securities class action asserting claims under Sections 10(b) and
7 20(a) of the Securities Exchange Act of 1934 (the “Exchange Act”), and SEC Rule 10b-5
8 promulgated thereunder (17 C.F.R. § 240.10b-5), on behalf of all persons and entities
9 who purchased or acquired publicly traded securities of Twitter from August 3, 2020
10 through August 23, 2022, both dates inclusive (the “Class Period”), and who were
11 damaged thereby.
12
13

14 2. In 2011, Twitter signed a consent order with the Federal Trade Commission
15 (“FTC”) through which it agreed to use industry-standard cybersecurity and privacy
16 protections. After a surprising July 2020 hack in which a teenager managed to
17 compromise the accounts of numerous politicians and celebrities, Twitter hired Peiter
18 “Mudge” Zatko, a renowned cybersecurity expert, to shore up its defenses. For more
19 than a year, Zatko brought deficiency after deficiency to Defendants’ attention, showing
20 Twitter had made essentially no progress since the FTC consent order. Some of these
21
22
23
24

25 ¹ Unless otherwise noted, all emphases are added. All facts attributed to Zatko are
26 drawn from his two whistleblower reports, the exhibits thereto, and his oral and written
27 testimony. These materials are all available at
28 [https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-
twitter-whistleblower](https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower) .

1 deficiencies were so obvious that Defendants must have known of them; Defendants
2 admitted to Zatko that they had known of others he unearthed. Yet before and even after
3 Zatko's warnings, Defendants continued to misleadingly boast of Twitter's cybersecurity
4 to investors. Defendants also boasted that unlike other software companies, its measure
5 of daily active users did not include users who were shown no ads; in fact, almost a third
6 saw no ads and earned Twitter no revenues. When the truth concealed by Defendants'
7 false statements was revealed, investors suffered significant losses.
8

9
10 3. In 2011, Twitter entered into a consent order with the FTC (the "FTC
11 Consent Order"). Twitter had permitted too many of its employees to have access to too
12 many employees allowing hackers to gain access to customer accounts by corrupting any
13 one of a host of Twitter employees. Through the 20-year FTC Consent Order, Twitter
14 agreed to adopt cybersecurity and privacy protections customary for a company of its
15 size and complexity, subject to stiff penalties if it failed to.
16
17

18
19 4. In July 2020, a teenager hacked Twitter, gaining widespread access,
20 including the ability to control accounts of his choosing. The teenager then tweeted scam
21 links from some of Twitter's most prominent accounts, including that of former
22 President Barack Obama.
23

24 5. The teenager's hack had outsized impact on Twitter. It froze thousands of
25 prominent accounts and paused hiring for a month.
26
27
28

1 6. Twitter was eager to create the perception that the teenage hack was a one-
2 time mistake that it had quickly addressed. A September 2020 article quoted Agrawal as
3 saying that Twitter had substantially tightened access to data. It also touted its hiring of a
4 world-renowned cybersecurity expert: Peiter “Mudge” Zatko.
5

6 7. Its publicity campaign complete, Twitter returned to touting its purported
7 protection of and commitment to cybersecurity and privacy:
8

9 a. It has “internal detection and monitoring tools that help alert us of
10 unusual behavior”;

11 b. Its internal “access is limited and is only granted for valid
12 business reasons (i.e., ensuring an account holder can get support
13 if they are locked out of their account)”;

14 c. It “give[s] people the ability to make a variety of choices about
15 their data privacy, including limiting the data we collect,
16 determining whether they see interest-based advertising, and
17 controlling how we personalize their experience.”
18

19 8. All these statements were false.
20

21 9. Zatko began work in November 2020. He spent the next two months
22 investigating the scope of Twitter’s problems. They were grave. In a February 2021
23 meeting, Zatko told Twitter’s senior executives—including at minimum Defendants
24 Dorsey, Agrawal, and Gadde—that they should be “alarmed”.
25
26
27
28

1 10. Zatko then laid out all the reasons why. First, its access controls were wildly
2 overpermissive: ***All*** Twitter’s engineers had access to ***all*** its source code and mounds of
3 customer data. Almost uniquely among large technology companies, it had never created
4 a separate “sandbox” where engineers could develop and test software before releasing it
5 into the world, so those engineers worked on live production systems with client data.
6 Nor could Twitter even catch internal intruders after the act, because it did not log
7 engineers’ access to data. Neither was Twitter’s software up to snuff: almost half of its
8 servers ran outdated software—in violation of Twitter’s policy—including in some
9 cases, software that was no longer being maintained by the vendor. These cybersecurity
10 deficiencies violated the FTC Consent Order.
11

12 11. Zatko laid out the consequences Twitter was already suffering. Twitter had
13 experienced 40 incidents, including 20 data breaches, in 2020, 70% and 90% of which
14 were linked to overpermissive access. Zatko told attendees “we are almost guaranteed to
15 have an access control-related breach and the problem is systemic.” Twitter concealed
16 these incidents from the public, though its internal records showed that the data of 200
17 million users and 20,000 employees were exposed.
18

19 12. The problem of poor technology was existential: as Zatko told attendees,
20 Twitter’s infrastructure was so bad that a cascading failure among its data centers could
21 permanently knock out Twitter. It very nearly did in spring 2021. Hundreds of engineers
22 sweated as they watched Twitter’s data centers come down one after the other. Upon
23
24
25
26
27
28

1 learning of the near-collapse at an *ad hoc* meeting, a Twitter director said “[i]sn’t this
2 exactly what [Zatko] warned us about?”

3
4 13. Zatko was concerned that these findings should be reported to Twitter’s
5 Board because they were alarming. Twitter’s executives were also alarmed, but for that
6 same reason, they obstructed Zatko from reporting the vulnerabilities to the Board. In
7 this particular instance, Defendant Gadde told Zatko not to supply a written report to the
8 Board and only go over his findings at a high level of generality.
9

10 14. Until his firing in January 2022, Zatko reported a steady stream of
11 deficiencies to Defendants, who ignored or marginalized him:
12

- 13 a. Zatko hired a consulting firm to create a report on Twitter’s
14 capacity to fight mis- and dis-information. Twitter authorized the
15 project, but when executives learned that a May or June 2021 draft
16 of the report had slammed Twitter and highlighted numerous
17 flaws, they instructed the firm to stop communicating with Zatko
18 directly and instead send it to an outside law firm which would
19 cleanse it of any bad facts before Zatko saw it. Twitter’s counsel
20 told Zatko this was intended to hide the findings and prevent them
21 from becoming known, even internally;
22
23
24
25
26
27
28

- 1 b. In August 2021, Zatko notified Agrawal that Twitter’s internal
2 engineering system was registering a huge number of failed
3 logins, likely a sign of hackers. Agrawal refused to investigate;
4
5 c. Contrary to industry cybersecurity standards, Twitter had no
6 uniform process to develop software, yet Twitter’s executives had
7 told Twitter’s Board that it had one. So when Zatko told the Board
8 as much, a board member noted that for years he had been hearing
9 “the effort was getting closer to being complete.” Soon after the
10 meeting, a Twitter executive called Zatko to tell him Agrawal was
11 upset with him for informing the Board; and
12
13 d. Twitter had no way to delete user data when they deactivated their
14 accounts because it only managed data sets containing 20% of its
15 data. The rest was uncategorized and could easily be misused by
16 Twitter employees who did not know what it was for or what
17 representations Twitter had made to obtain it.
18
19
20
21

22 15. Distressingly, when Zatko unearthed cybersecurity deficiencies, he was
23 frequently told that Twitter already knew about it and had decided to ignore it and hope
24 for the best. Zatko learned that contrary to its policy, Twitter was letting the corps of the
25 Indian Army responsible for operations in Kashmir run an influence operation that,
26 among other things, targeted reporters. When he reported it up, he was told Twitter
27
28

1 *already knew* about the campaign but had made an executive decision to tolerate it to
2 appease India's ruling party—even as Defendants told investors that “we’ve been very,
3 very transparent about any attempt that we’ve seen from state actors to manipulate the
4 conversation on Twitter, right? And we’ve shared those transparently.” He learned that
5 Twitter was potentially facilitating the Chinese government’s efforts to target dissidents,
6 both at home and abroad. They knew about that too, but were too dependent on revenue
7 from ads from Chinese companies, oddly since Twitter is blocked in China. Twitter
8 executives’ efforts instead focused on making the collaboration more palatable to its
9 employees—all while telling investors that its “policies are built primarily around the
10 promotion and protection of three fundamental human rights, freedom of expression,
11 safety, and privacy [] prioritizing safety above all others.” He learned that Twitter had
12 used unlicensed data to develop its algorithm. Defendants knew that, too, misled the
13 FTC about it, and misleadingly warned investors of three long paragraphs’ worth of
14 intellectual property risks while concealing that its key products were built upon stolen
15 intellection property.

16
17
18
19
20
21
22 16. Even as Zatko discovered more and more problems, the picture Twitter’s
23 executives presented to its Board grew rosier and rosier. Though Zatko attempted to
24 blow the whistle to the Board, Agrawal fired him before he could complete his report.
25 Ultimately, Twitter paid \$7.75 million to settle Zatko’s claims over his termination.
26
27
28

1 17. Twitter also misled investors about the prevalence of bots and spam
2 accounts. Twitter devised a metric, monetizable daily active users (“mDAU”), that
3 supposedly included fewer than 5% bots and spam accounts, yet in their public
4 statements, Defendants conflated mDAU with a measure of the total number of accounts.
5 More, mDAU itself was misleading, because a third of purportedly *monetizable* accounts
6 had never been *monetized*—not even a penny.
7

8
9 18. In April 2022, Twitter’s Board accepted a buyout offer from Elon Musk
10 (“Musk”). Yet the deal quickly soured.
11

12 19. On May 13, 2022, before the market opened, Musk tweeted out concerns
13 about Twitter’s representations concerning the number of bots. Twitter’s stock price fell
14 9.7% that day, falling another 8.2% over the next day as Musk continued to tweet his
15 concerns.
16

17 20. On July 7, 2022, the *Washington Post* reported that Musk had stopped
18 engaging in certain discussions around the deal. Twitter’s stock price fell 5.1%.
19

20 21. Then on July 8, 2022, Twitter publicly filed with the SEC a letter from
21 Musk terminating the deal, citing misrepresentations concerning the number of bots.
22 Twitter’s stock price plunged 11.3%.
23

24 22. Finally, on August 23, 2022, the *Washington Post* reported on the contents
25 of Zatko’s whistleblower disclosure and published a redacted version of his complaint.
26 In response, Twitter’s stock price fell 7.3%.
27
28

1 23. The next day, the Senate Judiciary Committee announced a hearing to air
2 Zatko's revelations.

3 24. Though Musk completed the buyout, Twitter is still living with the legacies
4 of the violations Zatko revealed—including an ongoing FTC investigation (coming mere
5 months after Twitter and the FTC signed a \$150 million settlement) and two
6 investigations by foreign government agencies.
7

8 **II. JURISDICTION AND VENUE**

9 25. The Counts asserted herein arise under and pursuant to Sections 10(b) and
10 20(a) of the Exchange Act (15 U.S.C. §§ 78j(b) and 78t(a)), and Rule 10b-5 promulgated
11 thereunder (17 C.F.R. § 240.10b-5).
12

13 26. This Court has jurisdiction over the subject matter of this action pursuant to
14 28 U.S.C. § 1331 and Section 27 of the Exchange Act (15 U.S.C. § 78aa).
15

16 27. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b)
17 and Section 27 of the Exchange Act (15 U.S.C. § 78aa). Twitter has offices in this
18 Judicial District, Defendants conduct business in this Judicial District, and a significant
19 portion of Defendants' acts alleged herein took place in this Judicial District.
20

21 28. In connection with the acts alleged in this complaint, Defendants directly
22 and indirectly used the means and instrumentalities of interstate commerce, including,
23 but not limited to, the mails, interstate telephone communications, and the facilities of
24 the national securities markets.
25
26
27
28

III. PARTIES

A. Plaintiffs

29. Court-appointed Lead Plaintiff William Baker, as set forth in the Certification previously filed in this action (ECF No. 28-2), acquired Twitter common stock at artificially inflated prices during the Class Period and was damaged when such artificial inflation was removed.

30. Additional Plaintiffs Mohammed Thaseen, Jill Sligay, Lenard Roque, and Amolkumar Vaidya, as set forth in Appendix A hereto (and, with respect to Mohammed Thaseen, as set forth in the Certification previously filed in this action (ECF No. 32-3))², acquired Twitter common stock at artificially inflated prices during the Class Period and were damaged when such artificial inflation was removed.

B. Defendants

31. Defendant Twitter, Inc. is a global social media platform. Twitter's stated goal is to be the place where the conversation is happening. Its users skew heavily towards academics, journalists, activists, and government officials, so it is more important than its relatively low number of users would suggest. During the Class Period, Twitter's common stock traded on the New York Stock Exchange ("NYSE") under the ticker symbol "TWTR."

² Mr. Vaidya's certification is forthcoming.

1 32. Defendant Jack Dorsey (“Dorsey”) co-founded Twitter and served two
2 stints as its Chief Executive Officer (“CEO”), the latter of which started before the Class
3 Period and ended November 29, 2021. Dorsey also served as a member of Twitter’s
4 Board of Directors (the “Board”) from May 2007 until May 25, 2022.
5

6 33. Defendant Parag Agrawal (“Agrawal”) served as the Company’s CEO from
7 November 29, 2021 until Musk’s acquisition of Twitter on or about October 27, 2022,
8 whereupon he was fired for cause. Agrawal worked at Twitter in engineering positions
9 beginning in 2011, including as its Chief Technology Officer from October 2017 to
10 November 2021.
11

12 34. Defendant Ned Segal (“Segal”) served as the Company’s Chief Financial
13 Officer (“CFO”) from June 2017 until Musk’s acquisition of Twitter, whereupon he was
14 fired for cause.
15

16 35. Defendant Vijaya Gadde (“Gadde”) served as Twitter’s Chief Legal Officer
17 since February 2018 and Secretary since August 2013, until Musk’s acquisition of
18 Twitter on or about October 27, 2022, whereupon she was fired for cause. Gadde joined
19 Twitter in July 2011 as Director, Legal until August 2013, then served as General
20 Counsel from August 2013 to February 2018 and as head of communications from July
21 2015 to August 2016.
22

23 36. Defendant Kayvon Beykpour (“Beykpour”) joined Twitter in 2015 when
24 Twitter acquired Periscope, a company founded by Beykpour that offered a live video-
25
26
27
28

1 broadcasting app. Beykpour led the Periscope team after that acquisition, and then
2 became Head of Product (sometimes referred to as “Product Lead”) in July 2018. In
3 December 2021, Beykpour was promoted to General Manager, Consumer, where he
4 oversaw the Product, Engineering, Design, Research, and Customer Service and
5 Operations teams. On May 12, 2022, Agrawal announced that Beykpour was leaving the
6 Company.
7

8
9 37. Dorsey, Agrawal, Segal, Gadde, and Beykpour are collectively referred to
10 herein as the “Individual Defendants.”
11

12 38. Twitter and the Individual Defendants are collectively referred to herein as
13 the “Defendants.”
14

15 **C. Relevant Non-Parties**

16 39. Peiter “Mudge” Zatko was employed by Twitter as Security Lead, a
17 member of the senior executive team responsible for Information Security, Privacy,
18 Physical Security, Information Technology, and Twitter Service (the corporate division
19 responsible for global content moderation enforcement) from November 16, 2020, until
20 the morning of January 19, 2022, when Defendant Agrawal abruptly terminated him as
21 he was preparing a whistleblower report. Before joining Twitter, Zatko held senior
22 positions at Google and Stripe, and within the Department of Defense, where he was
23 authorized to access Top Secret/Special Compartmented Information for work on
24 programs in both offensive and defensive cyber operations. Zatko has been formally
25
26
27
28

1 recognized for his qualifications and achievements by the Central Intelligence Agency,
2 the White House, and the U.S. Army, and the Office of the Secretary of Defense
3 bestowed upon him the Exceptional Public Service Award, the highest medal honor
4 available to civilian, non-career officials. On January 6, 2021, after the attack on the
5 Capitol, the incoming administration offered Zatzko the position of Chief Information
6 Security Officer for the United States, which he declined to continue to work at Twitter.
7

8
9 40. As discussed further herein, months after his termination, following
10 extensive correspondence with Twitter, Zatzko—through counsel—delivered extensive
11 whistleblower disclosures to the SEC, the FTC, the U.S. Department of Justice (“DOJ”),
12 and Congress, detailing Twitter’s extensive cybersecurity failures, cybersecurity
13 breaches and incidents, and misrepresentations to shareholders, regulators, and the
14 public.
15
16

17 41. Elon Musk is a Silicon Valley businessman and billionaire. Among other
18 things, he is the CEO of Tesla, Inc. On April 14, 2022, Musk made an unsolicited offer
19 to purchase Twitter for \$54.20 per share of common stock, or approximately \$44 billion.
20 On April 25, 2022, Twitter’s Board unanimously resolved to accept Musk’s offer,
21 subject to shareholder approval.
22
23

24 42. The United States Senate Committee on the Judiciary (the “Senate Judiciary
25 Committee”) is a standing committee of twenty-two U.S. senators whose role is to
26 oversee DOJ and review pending legislation, among other responsibilities. The Standing
27
28

1 Rules of the Senate confer jurisdiction on the Senate Judiciary Committee regarding
2 certain topical areas, including proposed legislation concerning internet privacy.

3
4 **IV. SUBSTANTIVE ALLEGATIONS**

5 **A. Twitter's Repeated Security and Privacy Incidents Lead to an FTC**
6 **Consent Order.**

7 43. Twitter was launched in 2006. Since inception, Twitter has collected
8 extensive information about its users, including for example login credentials, contact
9 information, contacts, messages, ad-trackers, the IP addresses the users employed and
10 the IP addresses' geolocation, and the browser and device used to log-in. Public
11 information including name, contact information (including phone numbers and current
12 and former email addresses), private messages, and other information is available,
13 including the user's non-public ring of "friends." Because many users re-use passwords
14 and logins, the data can also be used to hack into users' email accounts or used for
15 financial fraud. This information can also be useful for surveillance, including by
16 governments who are targeting activists.
17

18 44. In 2011, the FTC filed a complaint against Twitter concerning its failure to
19 properly protect this non-public consumer information.³ The complaint alleged that,
20 from 2006 to 2009, far too many Twitter employees—far more than proper cybersecurity
21 policies would accept—could exercise administrative control (referred to internally as
22

23
24
25
26
27 ³ See [https://www.ftc.gov/sites/default/files/documents/cases/2011/03/](https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf)
28 [110311twittercmpt.pdf](https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf).

1 “God Mode”) over Twitter’s internal systems and user data. A user in God Mode can
2 post, edit, and delete tweets from any user account, and access internal data concerning
3 any user. These included Twitter employees who did not need such widespread access
4 to perform their job functions. The individuals with this administrative control
5 numbered far above industry and security standards. Thus, unauthorized access to any
6 one of thousands of employee accounts could compromise Twitter’s entire platform.
7

8
9 45. Taking advantage of Twitter’s poor access controls, between January and
10 May 2009, at least two intruders obtained administrator-level access to engage in further
11 unlawful conduct.
12

13 46. Twitter entered into a consent order in March 2011 (the “FTC Consent
14 Order”), which remained in effect at all relevant times.⁴ The FTC ordered Twitter to
15 “establish and implement, and thereafter maintain a comprehensive information security
16 program that is reasonably designed to protect the security, privacy, confidentiality, and
17 integrity of nonpublic consumer information.” Components of this comprehensive
18 information security program included identifying security risks and preventing,
19 detecting, and effectively responding to cyberattacks. Twitter was required, inter alia, to
20 designate employee(s) to be accountable for the information security program and to
21 identify reasonably foreseeable security risks that could expose or compromise
22
23
24
25

26
27 ⁴ See [https://www.ftc.gov/sites/default/files/documents/cases/2011/03/](https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf)
28 110311twitterdo.pdf.

1 nonpublic consumer information, taking into account various considerations, such as
2 employee training and management, information systems, and prevention, detection and
3 responses to various system failures, such as attacks and account takeovers. Thus, the
4 FTC Consent Order required that Twitter adopt industry standard cybersecurity and
5 privacy protection protocols. The security program was to be regularly tested and
6 monitored to ensure the effectiveness of its key controls, systems, and procedures.
7

8
9 47. Twitter also agreed not to misrepresent “the security, privacy,
10 confidentiality, or integrity of any nonpublic consumer information”. The order
11 identified two specific types of misrepresentations: those concerning its ability to “(a)
12 prevent unauthorized access to nonpublic consumer information; or (b) honor the privacy
13 choices exercised by users”.
14
15

16 48. The order also imposed various reporting requirements upon Twitter to
17 ensure it was keeping the FTC informed of its progress on its security system for ten
18 years following issuance of the order. The Consent Order itself would expire on March
19 2, 2031.
20

21 49. In the years since the FTC Consent Order, Twitter has grown substantially,
22 from 138 million monthly active users in 2012 to 450 million in 2022, and from \$317
23 million in annual revenue in 2012 to over \$5 billion in 2021.
24
25

26 50. But as Twitter has grown, so has the severity of the sanction it can expect if
27 the FTC catches it violating the Consent Order. In 2012, Facebook entered into a
28

1 consent order with the FTC concerning its privacy promises to consumers. That order
2 required Facebook to institute substantial changes to its data privacy and security
3 practices. When the FTC found in 2020 that Facebook had violated the order, it imposed
4 a \$5 billion fine.
5

6 **B. In 2020, Twitter Experiences a Major Cybersecurity Incident.**

7
8 51. In July 2020—following nine years of supposed fixes, investments,
9 compliance policies, and reports to the FTC by Twitter—Twitter was hacked by a
10 seventeen-year-old recent high school graduate and his friends. The hackers managed to
11 take over the accounts of former President Barack Obama, then-Presidential candidate
12 Joseph Biden, and high-profile business leaders such as Jeff Bezos, Bill Gates, and
13 Musk. The hackers then tweeted from the accounts urging the accounts' followers to
14 send Bitcoin cryptocurrency to an account the hackers had created.
15
16

17 52. The hack was one of the most visible successful cyberattacks, and it
18 triggered a global security incident, in particular because it involved the account of a
19 former U.S. President.
20

21 53. To mitigate the risk of continued propagation, Twitter imposed a days-long,
22 system-wide shutdown of system access to all of its employees. For about a month,
23 Twitter paused hiring and shut down many basic operations.
24

25 54. In fact, the hack was remarkably unsophisticated: the teenage hackers
26 simply called some Twitter employees and asked them for their passwords. A few
27
28

1 employees were duped and complied. Because of Twitter’s systematic practice of
2 granting more employees more access than necessary, those credentials gave the hackers
3 access to “God Mode”, letting them tweet from any account they wanted.
4

5 **C. In 2020, the FTC Takes Further Action Against Twitter**

6 55. On July 28, 2020, Twitter was served by the FTC with a draft complaint
7 alleging that it had violated the 2011 Consent Order, which Twitter announced on
8 August 3, 2020. The FTC charged that from 2013 to 2019, Twitter misused users’ phone
9 number and/or email address data for targeted advertising even though Twitter solicited,
10 and users provided, this information for safety and security purposes only (e.g., for dual-
11 factor authentication of user log-in attempts).
12
13

14 56. The FTC would later impose a \$150 million fine against Twitter for the
15 misconduct alleged in the draft complaint. The FTC’s close interest further showed that
16 Twitter’s compliance with the FTC Order was material.
17
18

19 **D. Twitter Recruits Zatzko as Security/Integrity Lead.**

20 57. Defendants set out to reassure investors that they had quickly overcome the
21 problems that led to the hack. Acknowledging that over-permissive settings were the
22 cause, Agrawal told *Wired* for a September 28, 2020, article that “[t]he amount of
23 access, the amount of trust granted to individuals with access to these tools, is
24 substantially lower today.”
25
26
27
28

1 58. Defendant Dorsey, then Twitter's CEO, also recruited Zatkan. Zatkan started
2 work at Twitter on November 16, 2020 as its Security/Integrity Lead. Presumably at
3 Twitter's request or at least with its permission, Zatkan gave *Reuters* an exclusive
4 interview to announce the hiring. When *Reuters* published an article based on the
5 interview, Dorsey tweeted it out on his own account.
6

7
8 **E. Zatkan Becomes a Whistleblower**

9 59. Zatkan stayed at Twitter through January 2022. During his time, he
10 consistently raised alarms about Twitter's cybersecurity. He reminded all Defendants
11 that half of Twitter's employees had access to all of its source code and customer data
12 and that Twitter had no way of tracking their access; that Twitter knowingly employed
13 agents of foreign governments, including adversaries of the United States and
14 governments with deplorable human rights records; that more than half of Twitter's
15 datacenter servers, and almost a third of its laptops, were out of date and vulnerable to
16 hacks; that Twitter did not come close to complying with the FTC Consent Order; and
17 that Twitter might not be able to ever resume operations if enough of its datacenters
18 failed at once.
19
20
21
22

23 60. On January 19, 2022, Agrawal fired Zatkan after the latter attempted to
24 inform the Risk Committee of the Board that Twitter was not making significant
25 progress on cybersecurity.
26
27
28

1 61. In June 2022, Twitter paid Zatko \$7.75 million to settle his claims of
2 unlawful termination, or more than the total cash compensation it paid to its six named
3 executive officers in 2021.
4

5 62. On July 6, 2022, Zatko filed an 84-page, 116-paragraph whistleblower
6 complaint with the SEC, FTC, and DOJ, and a separate whistleblower complaint with
7 the Senate Judiciary Committee.
8

9 63. On August 23, 2022, the *Washington Post* published a redacted version of
10 Zatko's complaint along with two internal Twitter documents attached as exhibits
11 thereto.
12

13 64. On August 24, the Senate Judiciary Committee announced that it had
14 arranged for Zatko to testify at hearing that would take place on September 13, just three
15 weeks later. In short order, two more foreign regulators announced that they were
16 investigating Twitter. The FTC also started an investigation, which is ongoing.
17
18

19 **F. Zatko at Twitter**

20 65. When Zatko arrived at Twitter, Dorsey assigned him a wide portfolio, with
21 hundreds of staff and thousands of contractors in chains that reported up to him on topics
22 including: Information Security (protecting the integrity and security of all Twitter
23 systems and data); Privacy (creating, maintaining, and enforcing privacy policies and
24 processes, plus engineering and executing them across all Twitter systems and data, to
25 avoid liability with the FTC and build systems and processes that respect people's data);
26
27
28

1 Corporate Security (protecting the physical security and safety of employees, offices,
2 and data centers); Information Technology (overseeing the internal systems for finance,
3 HR, and internal corporate technologies and communications); and “Twitter Service,”
4 the division tasked with operational enforcement of global content moderation at scale,
5 including processing and the removal of various spam and spam bots.
6

7
8 66. Upon joining Twitter, Zatko spent two months performing an in-depth
9 evaluation of these areas, interviewing about 40 employees, from members of the
10 executive team to engineers to salespeople. Zatko attended engineering meetings,
11 reviewed internal technical documents, and directly evaluated some of Twitter’s key
12 computer systems and servers.
13

14
15 67. Zatko’s findings following his two-month study were dire. After nearly a
16 decade of explosive growth, Twitter had made little meaningful progress on basic
17 security, integrity, and privacy systems, in violation of the FTC Consent Order. Years of
18 regulatory filings in multiple countries were misleading. Indeed, Twitter had
19 haphazardly expanded into contentious international areas without even following the
20 weak corporate policies it had in place.
21

22
23 68. Zatko’s reports, all highly-experienced experts who were intimately familiar
24 with Twitter’s problems with the FTC, told Zatko unequivocally that Twitter had never
25 been in compliance with the Consent Order, and was not on track to ever achieve full
26 compliance. Early in his tenure, Zatko heard Defendant Agrawal tell the executive team
27
28

1 that “Twitter has 10 years of unpaid security bills,” meaning that Twitter had declined
2 for a decade to invest in security.

3 69. Zatko promptly communicated his findings to Defendants. He would
4 continue to do so until his January 2022 termination.

5
6 *1. February 2021 Executive Meeting*

7 70. Having concluded his investigation, Zatko delivered a presentation to
8 Twitter senior executives in February 2021, to prepare for the presentation of Q1 2021
9 results executives would deliver to the Board about a week later. Both Dorsey and
10 Agrawal attended the meeting. Gadde and Beykpour were frequent attendees at such
11 executive meetings. Moreover, Zatko was instructed at Gadde’s direction not to create a
12 draft presentation for the Board, showing Gadde had knowledge of Zatko’s presentation.
13

14 71. Zatko began ominously. According to his prepared notes, Zatko stated in his
15 introduction that: “You should be alarmed. It doesn’t need to be this bad.”
16

17 72. At the meeting, Zatko showed why Defendants “should be alarmed”. Zatko
18 began by noting that in 2020 Twitter had experienced 40 incidents, including 20 data
19 breaches, many of which required reporting to the FTC. Respectively, 70% and 90% of
20 the security incidents and data breaches were related to access controls.⁵ As a result,
21
22
23
24
25

26 ⁵ Twitter need only report securities incidents to the FTC if sensitive user
27 information—such as emails, passwords, phone numbers or users’ credit card data—
28 was exposed.

1 Zatko explained, “we are almost guaranteed to have an access control related breach and
2 the problem is systemic.”

3 73. Access controls were a particularly important subject for Twitter because
4 overbroad access was the source of both the 2011 Consent Order and the draft complaint
5 the FTC had served in June 2020. That Twitter’s access controls were even worse ten
6 years after the FTC Consent Order created enormous legal risks.
7

8 74. The number of incidents and breaches Twitter suffered was wildly out of
9 proportion to Twitter’s size and complexity. Zatko later told the Board that based on his
10 extensive experience, Twitter should suffer at most 1 incident per quarter, or one tenth as
11 many as Twitter in 2020.
12

13 75. The consequences were undisclosed and substantial. As Zatko explained,
14 the data of previous Twitter employees, contractors, and users—some 200 million users
15 and 20,000 employees—was exposed as a result of security incidents just in 2020 alone.
16

17 76. Zatko then reported *why* Twitter’s suffered so many incidents and breaches.
18 For one, Twitter’s servers were not secured. As Zatko explained, 53% (186,372) of
19 Twitter’s data center servers were running out-of-date operating systems. In many cases,
20 the operating system was no longer supported by the vendor, such that it was unlikely
21 that bugs (including those affecting security) would be identified and fixed.
22
23
24
25
26
27
28

1 77. Twitter violated the FTC Consent Order because out-of-date operating
2 systems are an important vulnerability; indeed, Twitter’s own engineering standards
3 demanded that operating systems be fully up to date.
4

5 78. Zatko then recounted that Twitter did not impose any controls over what
6 software its employees could install on their work systems. Nor could it tell what
7 software these employees actually had installed, because Twitter had an “[e]stimated
8 10% visibility across [its] systems, services, and clients (laptops and phones)”. Twitter
9 thus had no way to determine whether thousands of employee devices used to connect to
10 Twitter’s systems contained spyware or were otherwise compromised.
11
12

13 79. Zatko also highlighted Twitter’s over-permissive access controls. As a rule,
14 software companies maintain “quality assurance” platforms, a sort of sandbox where
15 new code and application updates can be safely integrated and tested without any impact
16 on the live “production” systems environment, the platform used by customers. As Zatko
17 reported, however, Twitter did not have a sandbox. Instead, Twitter’s engineers worked
18 directly in Twitter’s Production environment with live customer data.
19
20

21 80. The practice was a huge red flag for job candidates, who frequently
22 expressed disbelief. One particular candidate for Vice President of Information
23 Technology considered withdrawing his application because Twitter’s lack of basic
24 engineering hygiene in their arrangement presaged major headaches. The practice is
25
26
27
28

1 almost unheard of at modern tech companies, caused repeated problems for Twitter, and
2 violated the FTC Consent Order which called for Twitter to employ industry standards.

3
4 81. As Zatko explained, not only did the lack of a sandbox create risks to
5 Twitter's operations, it also meant that Twitter granted overbroad access to the
6 production environment to every engineer, as it was the only place where Twitter
7 engineers could build and test new code. And indeed, at the time, 43% of Twitter's full-
8 time employees (2,662 in total) had access to its full production system, including
9 Twitter's full source code, and customer data.
10

11
12 82. Zatko also explained that Twitter's employees had access to other sensitive
13 databases. More than 1,000 had access to advertiser information, likely including bank,
14 routing, and account information.
15

16 83. This was not a new problem. Zatko's notes for his presentation concerning
17 overbroad access indicate that this information "ha[d] been raised to the board before
18 (perhaps without stats)".
19

20 84. It was not just current employees who posed a problem. Zatko told
21 attendees that in 2020, Twitter knew of a total of 1,477 (full time employee) and 10,357
22 (contractors) person-days⁶ in which departing employees still had full internal access to
23 systems and data.
24

25
26
27 ⁶ "Person-days" here is the sum of each day a departing employee had full internal
28 access. Thus, if three employees each had full access for one day, there were three person-days.

1 85. What made accessing data even more attractive was that employees were
2 almost guaranteed not to be caught because Twitter also coupled its massively overbroad
3 access with poor tracking of what was accessed. Zatko had been told in his investigation,
4 and reported in the February 2021 presentation, that Twitter had no centralized logging
5 of the actions of its employees. That means that Twitter would not know if an employee
6 inappropriately accessed data. Zatko would later testify as much in response to a
7 question from the Senate Judiciary Committee:
8

9 If a Twitter employee had access to main systems and inappropriately
10 accessed user data, would Twitter have any way to know that this occurred,
11 what data was accessed, or what was ultimately done with that data?
12

13 ANSWER: *In general no.* There was insufficient logging (and/or
14 insufficient monitoring of logs), a lack of awareness of data, and
15 inappropriate access control. While there may be certain situations where
16 Twitter could know these things they were the exception rather than the
17 norm. I feel confident in this response because of multiple times where it
18 was necessary to understand what had happened on certain systems, or who
19 had accessed or created particular data and I was repeatedly informed that it
20 was unknown and that there were no ways to figure out the answer to such
21 questions.⁷

22 86. Leaking was not just theoretical; as Zatko reported at the February meeting,
23 he had been told that “leaking is the norm.”
24

25 ⁷ The “certain situations” Zatko cites appear to refer to a Twitter internal tool, Guano.
26 Guano logs activities of specific Twitter employees when they use specific Twitter
27 tools. It does not log access using all of Twitter’s tools, nor does it log access when an
28 insider does not use a Twitter tool. As Zatko put it in a July 20, 2021 text to Defendant
Segal, “[a]ny engineer could figure out how to [obtain customer information] under the
hood without needing to use [any Twitter] tools.”

1 87. Finally, Zatko highlighted a “surpris[ing]” “existential threat”. As he told
2 attendees, it was not uncommon for Twitter engineers’ bad software pushes to cause
3 some of its datacenters to fail. And all of Twitter’s engineers had access to the
4 datacenters. So it was possible, maliciously or inadvertently, for all of Twitter’s
5 datacenters to fail at once. Yet Twitter had no viable recovery plan for this contingency.
6 Even after the data centers recovered, it could take weeks or months to restore Twitter.
7 Twitter might even be permanently disabled.

8
9
10 88. Zatko expected to provide a written report to the Board. Yet according to
11 Zatko, Defendant Gadde, told Zatko through a subordinate not to send Twitter’s Board a
12 detailed written report but instead to convey his findings orally and only at a high level
13 of generality.
14

15
16 89. Falling far behind industry practice was not, for Twitter, a mere competitive
17 disadvantage. It was a violation of the FTC Consent Order. Thus, these deficiencies
18 foretold trouble with the FTC.
19

20 90. As 2021 progressed, Zatko raised more and more concerns with Twitter’s
21 management. Yet Defendants obstructed his attempts to address or raise problems.
22

23 91. The problems Zatko raised were not trivial. They regularly alarmed Twitter
24 directors. For example, in or about Spring 2021, Twitter’s primary data center began
25 experiencing problems from a runaway engineering process. Twitter moved operations
26 to other systems outside of this data center. These data centers could not handle the rapid
27
28

1 changes. They began failing. According to Zatko, hundreds of engineers watched the
2 data centers struggle to stay running. Twitter's head of engineering insisted that the
3 Board of Directors be informed of the looming catastrophe. The Board was shocked.
4 Board Member Robert Zoellick responded in Zatko's presence, that "[i]sn't this exactly
5 what [Zatko] warned us about?"
6

7
8 92. Twitter engineers had to work around the clock and only stabilized the
9 problem shortly before a complete shutdown. This incident was not publicly disclosed.
10

11 93. The problems persisted. During 2021, according to Zatko, Twitter had a
12 "near continuous number of security and privacy incidents", nearly two-thirds of which
13 were caused by access control issues.
14

15 94. Zatko raised these problems with Defendants. For example, beginning mid-
16 2021, Zatko initiated bi-weekly one-on-one meetings with Agrawal. Zatko used these
17 meetings to, among other things, flag cybersecurity issues.
18

19 95. And some Defendants subjectively believed that Twitter's policies were
20 dangerous. For instance, according to Zatko, after receiving quantified data showing
21 Twitter's alarming performance on one privacy issue, Defendant Gadde responded in
22 sum and substance "so this proves that we haven't made any progress over the past four
23 years."
24
25
26
27
28

1 2. *Alethea report*

2 96. In early 2021, Zatko hired consulting firm Alethea Group to create a report
3 on Twitter’s capacity to combat mis- and dis-information, fight spam and hostile actors,
4 and promote overall platform integrity. In or around May or June 2021, Alethea
5 delivered to Zatko a devastating draft report. Among other things, the Alethea report
6 concluded that Twitter “operate[d] in a constant state of crisis that does not support the
7 company’s broader mission of protecting authentic conversation.” It “identified
8 significant gaps in resource allocation” leading to “reactive” policies and actions and an
9 organization that did not “think about emerging threats.” Thus, Twitter was “not
10 currently set up to deliver globally on trust and safety.”
11
12
13

14 97. The deficiencies the Alethea Report identified included:
15

- 16 a. The tools Twitter employed were “outdated, ‘hacked together’, or
17 difficult to use” and “lack[ing] in automation and sophisticated
18 tooling”;
19
20 b. Twitter’s staff lacked the ability to operate in the languages
21 Twitter users employed. “The [Information Operations, IO] team
22 has one staff member with expertise in Russia, one with expertise
23 in Iran, and one with expertise in China, making staffing and
24 coverage, particularly during a crisis, unsustainable”. It had “no
25
26
27
28

1 Japanese speakers on the Site Integrity team”⁸ *even though Japan*
2 *is Twitter’s second largest market;*

3
4 c. Twitter’s divisions were “siloed and not clearly defined” and
5 relied on haphazard “personal relationships” between
6 disconnected employees rather than “a formal organizational
7 structure”. Site Integrity depended on employees who “have no
8 accountability to Site Integrity” and act only out of “goodwill”,
9 with “data sources [] spread across several different systems and
10 requir[ing] largely manual processes to access and analyze”. With
11 different teams handling different issues, Twitter was unable to
12 respond effectively when an incident did not correspond clearly to
13 one team’s function;
14

15
16 d. Twitter lacked real-time monitoring capability (“one of the most
17 used tools, ClusterDuck, which identifies networks of similar
18 and/or coordinated accounts by country, does not do real-time
19 monitoring and analysis”);
20

21
22 e. Twitter implemented rapid policy changes in response to crises
23 without input from the relevant stakeholders; and
24
25
26

27
28 ⁸ Site Integrity is the Twitter division responsible for responding to misinformation.

1 f. Twitter did not learn from experience (“Twitter lacks sufficient
2 processes to measure progress and impact, and therefore fails to
3 implement lessons learned from the past”).
4

5 98. According to Zatko, when senior executives learned of the Alethea Report’s
6 conclusions, they attempted to bury it. Without notifying Zatko, some senior executives
7 approached Alethea Group and ordered them to enter into a contract with an outside law
8 firm. This new contract provided that Alethea would first send drafts to the law firm,
9 rather than Zatko. The law firm would remove factual information that would be
10 especially embarrassing for Twitter, and then return to Alethea Group a “clean” version
11 to present to Zatko. Even Alethea recognized that the request was facially improper:
12 Zatko testified that Alethea told him “[t]his does not feel right to us what’s going on.”
13 Confirming Alethea’s view, Twitter counsel told Zatko that this was intended to hide the
14 findings and prevent them from becoming known, even internally.
15
16
17
18

19 3. *Zatko Tells the Board Risk Committee Facts Showing that*
20 *Twitter Is Not Complying with the FTC Consent Order*

21 99. In its initial attempts to comply with the FTC Consent Order, Twitter had
22 decided to create a Software Development Life Cycle (“SDLC”) plan, which is a
23 uniform process to develop and test software. SDLCs set out the steps the company will
24 take to plan, design, define, build, test, and deploy new software. Implemented with
25 automated checkpoints, established application security standards, and security
26 architecture oversight, these standard processes deliver web and mobile applications that
27
28

1 meet technology industry security standards and are easily upgraded when new software
2 vulnerabilities are discovered. These steps help ensure software is safe and segregate the
3 development from production environments.
4

5 100. An industry practice standard recommended by International Standards
6 Organization (“ISO”)⁹ outlines technical implementation requirements for a secure
7 SDLC. It includes requirements for building security checkpoints into the SDLC, for
8 example: “[a] secure development policy should consider developers’ capability of
9 avoiding, finding and fixing vulnerabilities.” (ISO 27002-14.2.1.2-h) and
10 “[o]rganizations should establish and appropriately protect secure development
11 environments for system development and integration efforts that cover the entire system
12 development lifecycle”. (ISO 27002-2015, 14.2.6). That Twitter attempted to create an
13 SDLC in response to the FTC Consent Order demonstrates that Defendants understood
14 that an SDLC was an essential component of cybersecurity.
15
16
17
18

19 101. In or around May 2021, Zatko reported to Board’s Risk Committee that
20 Twitter only had a template SDLC rather than a functioning one, and that the template
21
22
23
24

25
26 ⁹ The ISO is an independent, non-governmental organization that develops and
27 publishes international standards in all technical and nontechnical fields other than
28 electrical and electronic engineering. The ISO is a highly reputable organization and
the standards it promulgates are authoritative.

1 had only been rolled out for roughly 8-12% of projects.¹⁰ More, the SDLC project
2 established by Twitter, called Flyaway, included none of the important technology
3 controls named above that are part of an SDLC.
4

5 102. The disclosure shocked the Risk Committee. Upon receiving Zatko's report,
6 Board Chair Patrick Pichette was incensed and noted that for years the Board had been
7 hearing "the [SDLC] effort was getting closer to being complete".
8

9 103. Soon after Zatko's report to the Risk Committee, a Twitter executive called
10 Zatko and stated that the executive and Agrawal were upset with Zatko over the
11 information that he had presented to the Risk Committee. Accordingly, Agrawal was
12 aware of the facts Zatko set out in his presentation.
13
14

15 4. *Twitter Violates the FTC Consent Order by Using Customer*
16 *Data for Purposes the User Had Not Consented to Even as It Is*
17 *Negotiating A Fine For Doing the Exact Same Thing*

18 104. Then, in mid-2021, Twitter's product sales team once again saw a data set
19 and, in the absence of any data tracking, just started using it for ad tracking without
20 determining whether the relevant users had consent to the use of their data for
21 advertising purposes or whether such use was otherwise permissible. That is the exact
22 violation identified in the 2020 FTC draft complaint. Upon learning of the violation, a
23
24
25

26 ¹⁰ According to Twitter's 2021 Proxy Statement, "[m]anagement regularly engages
27 with our full board of directors and our Risk Committee on Twitter's security and
28 privacy programs and their related priorities and controls."

1 Twitter executive stated “So we only started to address the problem, and then got side
2 tracked and forgot about it? We do that for everything.”

3
4 105. Twitter was at that moment negotiating the amount of a fine for improperly
5 using data in violation of customers’ consent, so Defendants knew the conduct violated
6 the FTC Consent Order.

7
8 5. *Failed Logins*

9 106. In or around August 2021, Zatko notified Agrawal that the login system for
10 Twitter’s engineers was registering, on average, between 1,500 and 3,000 failed logins a
11 day.
12

13 107. A failed login is recorded when a person gets his or her username or
14 password wrong when attempting to log in. Failed logins can occur when legitimate
15 users forget their password. But they can also be a sign that outsiders are trying to guess
16 passwords to log into Twitter’s systems.
17

18 108. Twitter had approximately 4,000 engineers at the time. It is questionable
19 that every day one third to two thirds of its engineers made a mistake in entering their
20 password. The high number of failed logins was a red flag that hackers may be targeting
21 Twitter.
22
23
24
25
26
27
28

1 109. At a minimum, the FTC Consent Orders directive to “monitor[] the
2 effectiveness of the safeguards’ key controls” required that Twitter investigate the logins
3 to determine whether they were hacking attempts.¹¹
4

5 110. So Zatko asked Agrawal to assign someone to diagnose why this was
6 happening and fix it. Yet Agrawal never assigned anyone at all to the project. Agrawal
7 did not even attempt to determine how frequently Twitter would expect to experience
8 failed logins.
9

10 6. *Log4j* 11

12 111. In December 2021, it was announced that there was a critical theretofore
13 unknown vulnerability in “Log4j.” According to the Department of Homeland Security’s
14 Cyber Safety Review Board,¹² “Log4j is a piece of open-source software that developers
15 have integrated into millions of systems. A vulnerability in such a pervasive and
16 ubiquitous piece of software has the ability to impact companies and organizations
17 (including governments) all over the world.” By exploiting the Log4j vulnerability,
18 hackers can remotely take control of a computer. The Department of Homeland
19
20
21
22
23

24 ¹¹ See, e.g., Justin Massey & Maxim Brown, *Best practices for monitoring*
25 *authentication logs*, available at <https://www.datadoghq.com/blog/how-to-monitor-authentication-logs/>; see also CrowdStrike, *Credential Stuffing*, available at
26 <https://www.crowdstrike.com/cybersecurity-101/credential-stuffing/>.

27 ¹² See [https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-](https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf)
28 [July-11-2022_508.pdf](https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf)

1 Security's Cybersecurity and Infrastructure Security Director stated that the Log4j
2 security flaw was the "most serious" she had seen in her career.

3
4 112. Researchers worked non-stop to develop a patch that fixed the vulnerability,
5 which they made available in late December. But because of its chaotic infrastructure,
6 Twitter was unable to thoroughly assess its exposure to Log4j or its remediation efforts.
7
8 For all Twitter knew, it had not addressed the Log4j vulnerability and remained critically
9 exposed. Nor would it be able to prove to the FTC's satisfaction that it had addressed
10 Log4j, as Twitter must to avoid hefty fines or even injunctions.

11
12 7. *Insecure software*

13 113. As Zatko had reported back in February 2021, Twitter did not monitor what
14 employees did with their computer workstations and did not prevent them from installing
15 programs. Further, key security settings could be disabled.

16
17 114. As a result, installed or modified software to make their jobs more
18 convenient. On or before December 2, 2021, Zatko learned that 3,060 of Twitter's 9,000
19 systems had disabled automatic software updates. Automatic updates are necessary to
20 patch bugs as they are detected. They are also required by Twitter's engineering
21 standards. Disabling automatic updates creates a risk that users will not fix disclosed
22 security vulnerabilities. Failing to update to address **known** vulnerabilities is particularly
23 risky because publicizing bugs and fixes to users also publicizes them to hackers. Then,
24
25
26
27
28

1 hackers race to exploit the bugs before they are patched. Any company that has not
2 patched its software is a soft target.

3
4 115. In other cases, employees deliberately installed spyware on their work
5 computers at the request of external organizations. Twitter learned of several instances,
6 but it did not proactively look for cases. Instead, it discovered the instances by accident
7 or because the employees had a change of heart and self-reported.

8
9 116. That Twitter allowed employees to haphazardly install new programs and
10 turn off automatic updates violated the FTC Consent Order because it fell below industry
11 standards. Indeed, it violated *Twitter's own* security policy.

12
13 117. In or around Q3 or Q4 2021, Zatko learned that no Twitter employee
14 computers were being backed up at all. Twitter's IT department had recognized the need
15 for a backup system, having managed one for years, but the system had never been tested
16 and was not functioning correctly. When they learned of the system's flaw, Twitter
17 executives expressed that it was a positive: without any backups, Twitter could not
18 respond to legitimate government requests that Twitter divulge which Twitter employee
19 had access to which data at certain times. As one executive put it, "this is actually a good
20 thing because it means [Twitter] cannot comply with [legal requests] and have less
21 exposure." These remarks were implemented as policy: instead of fixing or replacing its
22 backup systems, Twitter discontinued them.

1 8. *Agrawal Fires Zatko for Blowing the Whistle*

2 118. On November 29, 2021, Dorsey informed Twitter staff that he was stepping
3 down as CEO, and that his replacement would be Agrawal.

4
5 119. When Zatko attempted to tell the Board it was receiving inaccurate
6 information, Agrawal pushed him out.

7
8 120. In or about the first week of December 2021, a senior employee of the
9 company emailed Zatko a draft PowerPoint presentation and other materials that were to
10 be distributed to the Board of Directors before the December 9 meeting. These materials
11 would then be the basis for the presentation to the Board.

12
13 121. Zatko determined that the materials contained false and misleading
14 statements about the state of Twitter's information security and privacy.

15
16 122. Zatko immediately contacted CEO Agrawal and other senior staff, seeking
17 to correct the misinformation in the draft materials and/or stop their delivery to the
18 Board. While those discussions were progressing, and to help provide more focus on
19 privacy and security to Board members, Zatko substituted corrected summaries for the
20 package sent to the full Board before December 9.

21
22 123. Zatko flagged four broad problems that were improperly omitted or
23 presented in a misleading way:

- 24
25 a. The materials reported a misleading statistic that 92% of
26 employee computers had security software installed, implying
27
28

1 those computers were secure. In fact, a full 30% of employee
2 systems were reporting that they had disabled critical safety
3 settings such as software updates. Other critical flaws reported by
4 the software brought this number closer to 50%.

5
6 b. A graph misleadingly suggesting that Twitter was making
7 significant progress in reducing access to production systems,
8 though the underlying data showed that at the end of 2021, 51% of
9 the 8,000 thousand full-time employees had privileged access to
10 Twitter's production systems.
11

12
13 c. A graphic in the document showed only a subset of security
14 incidents, presented as if to encompass all security incidents.
15 Twitter's actual total number of security incidents in 2021 was
16 closer to 60. The misleading graphic also attributed only 7% of
17 incidents to access control, when in reality access control was the
18 root cause of 60% of security incidents.
19

20
21 d. SDLC (and related processes and compliance) was presented as
22 largely completed, instead of still in the initial planning phases.
23

24 124. At the December 9 full Board meeting, the inaccurate materials were not
25 shared because Zatko replaced the materials with a short, factual summary of the work
26 on Information Security and Privacy teams.
27
28

1 125. Zatko's summary showed that Twitter had made little or no progress
2 towards becoming compliant with the FTC Consent Order in 2021. It disclosed the facts
3 Zatko had discovered concerning software updates alleged in ¶¶114-16 and 123, among
4 other significant violations of Twitter security policies.
5

6 126. The summary also repeated some warnings Zatko had already delivered. He
7 reminded Board members of Twitter's "inability to delete data", which compounded the
8 "risk of inappropriate access or use of data."
9

10 127. The summary updated the Board on the proportion of servers running out of
11 date operating systems: during 2021, it had increased to 68%. As Zatko stated, "[t]hese
12 issues, clients and servers, represent systems that are vulnerable for exploitation and
13 represent a lack of hygiene that is difficult to justify externally." In other words, they are
14 blatant violations of industry standards and the FTC Consent Order.
15
16

17 128. The summary also advised the board that engineers had a copy of Twitter's
18 entire source code on their laptops and that the Company had no mobile device
19 management for employee phones, leaving Twitter with no visibility or control over
20 thousands of devices used to access core company systems. If an engineer's laptop was
21 stolen, the thief could have Twitter's entire source code. Using off-the-shelf software,
22 the intruder could scan the source code for vulnerabilities, and for example, sell the
23 vulnerabilities to a bad actor interested in obtaining information about Twitter users.
24
25
26
27
28

1 129. Thus, despite Twitter knowing at the time that governments were targeting
2 the cell phones of activists, journalists, and executives, Twitter lacked basic abilities to
3 identify or defend against such targeting.
4

5 130. Zatko indicated details would be provided in the Board Risk Committee
6 meeting on December 16, a week later.
7

8 131. In a call on or around December 12 with Agrawal, Zatko conveyed his
9 concerns about the upcoming Risk Committee meeting because a senior employee in the
10 company intended to present the misleading material to board members at Risk
11 Committee meeting on December 16, 2021. On the call, Zatko offered to rewrite the
12 problematic report intended for the Risk Committee meeting to ensure it was accurate
13 and complete. Agrawal told him not to correct the information and instead asked for time
14 to look into this issue further.
15
16

17 132. Agrawal called two days later. He said that the materials as they stood
18 would be presented to the Board Risk Committee on December 16, despite Zatko's
19 informing Agrawal that the information in the materials were materially misleading.
20
21

22 133. Zatko again offered to create corrected materials, but Agrawal told Zatko
23 not to do so. Agrawal instructed Zatko to, instead, send the inaccurate materials,
24 unchanged, to the Risk Committee, and then correct the inaccuracies presented to the
25 Board in real time—and without accurate written materials. Agrawal promised that he
26
27
28

1 would personally call the members of the Committee after the fact to help ensure they
2 were not misled, if Zatko so requested.

3
4 134. The Risk Committee received the misleading document before the meeting,
5 and the senior Twitter employee conveyed the same misleading information in a verbal
6 briefing during the main part of the meeting on December 16. During the meeting,
7 Twitter's Chief Privacy Officer and Distinguished Privacy Engineers sent written
8 unprompted messages stating that the presentations' statements concerning access
9 control were "not accurate" because they only referenced one subset of the problem,
10 which was "wildly different from overall." As to statements concerning how many
11 laptops were secure, they stated that "this is 'how many have endpoint software' not how
12 many are in a good state." Thus, these senior employees echoed Zatko's concerns.

13
14
15
16 135. Following Agrawal's instructions, Zatko tried to use his 2-minute time slot
17 to correct the misleading information provided. Soon after, Zatko emailed Agrawal to
18 accept his prior offer to personally reach out to the board members to correct any
19 remaining misstatements.
20

21
22 136. Agrawal reneged on his promise, telling Zatko he was "disappointed in
23 him."

24
25 137. On January 4, 2022, unable to get Agrawal to meet or talk about the topic,
26 Zatko sent an email describing the December 16 meeting as "at worst fraudulent".
27
28

1 138. Following Zatko’s reference to “fraud,” Twitter’s Chief Compliance Officer
2 initiated an internal investigation and interviewed Zatko on January 11, 2022. The
3 compliance team agreed that the information delivered to the Risk Committee was
4 inappropriate and inaccurate and that Zatko should write a report correcting the
5 misrepresentations.
6

7
8 139. On January 18, at 11:16am, following a request from Twitter’s Chief
9 Compliance Officer, Zatko confirmed in writing that he planned to provide corrected
10 materials for the Board “by the end of this week” (January 21) as part of the fraud
11 investigation. Less than two hours later, Agrawal emailed Zatko, and surprised him with
12 a request to do a call 45 minutes later with himself and Omid Kordestani, Chair of
13 Twitter’s Risk Committee.
14
15

16 140. During the meeting, Agrawal falsely stated he had been waiting for over a
17 month for Zatko to produce corrective materials, though he had told Zatko not to produce
18 such materials. When Zatko attempted to correct this false statement, Kordestani
19 interrupted and refused to let Zatko continue.
20

21 141. Agrawal then terminated Zatko on the morning of January 19, 2022.
22

23 9. *February 2022 report*

24 142. After his firing, Zatko completed his report. He submitted the report to
25 Twitter’s Board in February 2022, two days before Twitter filed its 2021 10-K.
26
27
28

1 143. The report reminded the Board that the problems Zatko had identified as
2 early as February 2021 had not gone away. They had worsened:

3 a. 51% of Twitter's employees now had access to Twitter's full
4 source code and customer data, compared to 46% in February
5 2021.

6 b. 68% of Twitter's server operating systems were out of date, in
7 violation of Twitter policy, compared to 53% in February 2021.

8 c. There were 50 security incidents in 2021, compared to 40 in 2020.
9 80% of the 2021 incidents were caused by Twitter's long-standing
10 problems of access control and security configuration/bugs. 11
11 incidents were so serious that they had to be reported to the FTC.

12 d. Zatko conservatively estimated based on his review to date of
13 information still available to him that 40% of Twitter's laptops
14 either had updates disabled (30%) or violated other important
15 Twitter security requirements (10%).¹³

16 e. Twitter still did not have an SDLC.

17 144. In his report, Zatko also explained at length and with particularity the
18 precise reason why the materials that had been presented at Twitter's December 16, 2021
19

20
21
22
23
24
25
26
27 ¹³ Of course, some of the laptops with updates disabled also violated other important
28 Twitter security requirements.

1 Risk Committee meeting had been misleading. Zatko also explained that Agrawal had
2 insisted that the presentation be delivered and prevented Zatko from correcting the
3 record.
4

5 *10. Zatko Raises Critical Deficiencies, Only to Learn that Twitter*
6 *Had Known of and Buried Them*

7 *a) Foreign Intelligence Operations by Regimes with Terrible Human*
8 *Rights Records*

9 145. In 2021, Zatko learned that Twitter knowingly retained agents of foreign
10 countries on its payroll.

11 146. That foreign governments had placed agents within Twitter was not a
12 surprise to Defendants. Indeed, in November 2019, two former Twitter employees were
13 charged with spying for the government of Saudi Arabia. What Twitter did not disclose
14 was that it knowingly harbored even more agents of foreign governments.
15

16 147. The Indian government's intelligence agency, the Research & Analysis
17 Wing, targeted Twitter in intelligence operations. For example, on or about May 24,
18 2021, members of an elite Delhi Indian police branch raided Twitter's offices in the
19 middle of the night during a pandemic lockdown. The raid's stated justification—that
20 police wanted to discuss why a tweet by the ruling party had been labeled "manipulated
21 media" with Twitter employees—was unbelievable on its face because the raid's timing
22 ensured there would be no employees to talk to. According to contemporaneous media
23 accounts, the police officers stayed in Twitter's office for approximately an hour, giving
24
25
26
27
28

1 the implausible excuse that it had taken them that long to figure out that there were no
2 employees present.

3
4 148. As a result of the May 2021 raid and the Indian government's harassment of
5 Twitter employees, Twitter agreed to hire two specific individuals demanded by the
6 Indian government as full-time employees.

7
8 149. Twitter easily determined that the employees were agents. One of them was
9 revealed to have a completely fabricated history, which Twitter discovered by running a
10 background check. Further, upon hiring, one of the two employees immediately
11 requested copies of any legal documents and strategies Twitter was preparing in a case
12 against the Indian government. These documents and that case had nothing to do with
13 the employee's role.
14
15

16 150. Zatko repeatedly raised these issues and told others it required a CEO-level
17 decision as to whether to continue serving the Indian market, including at least in a July
18 2021 text to Defendant Segal and in meetings taking place in September 2021.
19

20 151. On or around July 20, 2021, Defendant Segal asked Zatko to investigate a
21 purportedly suspicious series of tweets. In a July 20, 2021, text message, Zatko reported
22 to Segal that "[i]n a matter of seconds, to evaluate the account you flagged, we
23 intimately knew the individual. Phone numbers, where they lived, other accounts they
24 control, their non-public ring of 'friends', type of phone/computer, ... and more." Zatko
25 explained that the individual was not a threat; rather, the individual had apparently been
26
27
28

1 flagged by a hostile foreign state actor. Zatkan explained how foreign governments could
2 exploit Twitter: “Each time we want to expand into a new country, with a physical
3 presence, most countries will see us as an ability to monitor their ‘adversaries.’” With an
4 in-country office, “the foreign entity will quickly realize they have the keys to our
5 kingdom.” Zatkan added that “India is particularly worrisome” because, as Twitter knew,
6 the Indian government was targeting its critics “to silence these people and remove them
7 from the public conversation.” Zatkan even told Segal “[w]e believe the Indian
8 government has already planted a government agent within Twitter.” Zatkan concluded
9 that “[w]e are handing the keys to a surveillance apparatus that is intending on using our
10 platform against our own mission [s]ilencing and targeting and undermining the public
11 conversation.”

12
13
14
15
16 152. Second, Zatkan’s prepared notes for a September 23, 2021 Risk Committee
17 meeting included the following: “Every night I go to sleep worrying if India is already
18 using our internal information to identify, target, and kill people expressing opposition to
19 the government.” Zatkan’s notes indicate that he told the Risk Committee that “as long as
20 we are within India’s borders [we] are not able to mitigate,” and there was a “95%
21 [chance] we have an active [Indian government agent] insider.”

22
23
24 153. But the issue was repeatedly tabled and never addressed, with one executive
25 stating as to the second spy “if we already have one insider threat from the Indian
26 government why does it matter if we have more?”
27
28

1 154. Zatko learned that the prevailing attitude among executives was that Twitter
2 had to compromise to serve the Indian market because of the revenue at stake. In 2022,
3 there were approximately 24 million Twitter users in India. It was Twitter's third largest
4 market. Further, Twitter's penetration in India was miniscule and had room to grow.

5
6 155. Twitter also violated its own policies to cozy up to India's ruling party.
7 Twitter's policy is to publicly disclose attempts by state-linked entities to manipulate
8 Twitter and its users. Yet in or around August 2020, Twitter learned that the Indian
9 Army unit responsible for operations in Kashmir was running an influence operation
10 inside Twitter. In executive discussions taking place in or around August 2021, Zatko
11 learned that Twitter had made the executive decision not to disclose the operation in
12 order to curry favor with India's ruling party, while Twitter contemporaneously
13 disclosed influence operations by India's rival in Kashmir, Pakistan.
14

15
16
17 156. Zatko publicly revealed on August 23, 2022, that Twitter had knowingly
18 concealed an influence operation by the Chinar Corps, the Indian army unit responsible
19 for Kashmir. Twitter maintains a running list of accounts linked to state influence
20 campaigns, which it shares with partners who produce reports. According to a report by
21 one of Twitter's partners, the very next day, Twitter released a new dataset to its partners
22 which included 1,198 accounts that tweeted about India and Pakistan.¹⁴ Twitter's
23
24
25

26
27
28 ¹⁴ See Shelby Grossman et al., *My Heart Belongs to Kashmir: An Analysis of a Pro-Indian Army Covert Influence Operation on Twitter*, Stanford Internet Observatory,

1 partner's report suggested that the accounts were part of a campaign by the Chinar
 2 Corp.¹⁵ Twitter had let the China Corp run brutal, dangerous misinformation. For
 3 example, one of the accounts' bios claimed it was "Exposing the traitors who call them
 4 [sic] #Kashmiri but are working towards destroying #Kashmiriyat....!!!!!" and targeted
 5 journalists. Twitter's prompt disclosure after it was caught corroborates Zatko's claim
 6 that it knowingly and wrongly concealed the Indian state campaign.
 7
 8

9 157. Twitter was also vulnerable more subtle intelligence operations. During the
 10 Class Period, Twitter had approximately 80 engineers in India who, like all engineers,
 11 had default access to Twitter's production environment and user data. Because of
 12 Twitter's failure to fix design flaws in its system architecture, it did not and could not
 13 restrict the access of these 80 engineers and 2 foreign agents, or monitor their accounts
 14 for inappropriate activity.
 15
 16

17 158. These employees were potential points of failure because they were subject
 18 to threats of physical violence. Like many others, India's government turned local
 19 Twitter employees into hostages, harassing them and threatening them with jail time. In
 20 one case, a Twitter employee was summoned several times by the police, and repeatedly
 21 had his cell phone (which Twitter permits to access large amounts of sensitive Twitter
 22
 23
 24

25 available at [https://stacks.stanford.edu/file/druid:zs105tw7107/](https://stacks.stanford.edu/file/druid:zs105tw7107/20220921%20India%20takedown.pdf)
 26 [20220921%20India%20takedown.pdf](https://stacks.stanford.edu/file/druid:zs105tw7107/20220921%20India%20takedown.pdf).

27 ¹⁵ Among other things, the network's tweets were "consistent with the Chinar Corp's
 28 objectives, praising the work of the Indian Army in India-occupied Kashmir" and the
 Chinar Corps' official account was the seventh-most retweeted or mentioned account.

1 internal information) confiscated. Twitter was ultimately forced to bring the individual
2 for an extended stay in the U.S.

3
4 159. As Zatko put it, because employees become hostages, opening an office in
5 abusive countries was a “one-way ticket.” Several other countries, including Turkey,
6 Nigeria, and Russia, demanded that Twitter open regional offices with actual Twitter
7 employees who could similarly be held hostage. In March 2021, Twitter agreed to open
8 an office in Turkey.
9

10
11 160. Defendants were also aware that the government of China may be using
12 Twitter to catch dissidents. Twitter is not available in China. To view Twitter, persons
13 located in China must use a VPN, which is illegal under Chinese law and of concern to
14 the Chinese government. Nonetheless, many domestic Chinese companies and even
15 Chinese government entities advertised on Twitter, in part because Twitter actively
16 courted Chinese governments.¹⁶ Twitter executives were concerned that these advertisers
17 used click-through ads to identify potential dissidents, because on Twitter the ads gave
18 the advertiser the ability to collect information from the user that he or she may not
19 realize they are giving up, including information sufficient to identify activists and their
20 colleagues. Twitter also makes it easy for the Chinese government to engage in such
21 activities, because it does not enforce any policies limiting the information advertisers
22
23
24
25

26
27 ¹⁶ Fanny Potkin et al, How China became big business for Twitter, Reuters, available at
28 <https://www.reuters.com/technology/block-blue-ticks-how-china-became-big-business-twitter-2022-09-13/>

1 can collect, nor does it determine what data advertisers collect. Instead, it asks
2 advertisers to act responsibly and self-police.

3
4 161. According to Zatko, Twitter executives were concerned that the Chinese
5 entities would use the information to learn sensitive information about Chinese users.
6 Twitter executives knew that accepting Chinese money risked endangering Chinese
7 dissidents. Twitter understood this constituted a major ethical compromise. But Zatko
8 was told by the executive in charge of sales that Twitter was too dependent upon the
9 revenue stream from Chinese companies to do anything other than attempt to increase it.
10 The executive told Zatko that instead of addressing the problem, “we need something
11 that will make the employees more comfortable with the fact that we’re doing this.”
12
13

14
15 162. *Reuters* has reported that Twitter earns hundreds of millions of dollars a
16 year selling ads to China-based clients, guaranteeing that Twitter’s top officers were
17 involved.¹⁷
18

19 163. In January 2022, Zatko learned that an external source had even warned
20 Twitter that there was an agent of China’s intelligence services on its payroll, whom
21 Twitter did not immediately fire.
22

23 *b) False Statements to the FTC*

24 164. On or around January 13, 2022, Zatko was told that Twitter did not have
25 appropriate licenses for the training data it had employed to create core machine learning
26

27
28 ¹⁷ *Id.*

1 models. These models were a key part of Twitter's service. This means that owners of
2 the intellectual property may sue to shut down Twitter's business or demand substantial
3 damages.
4

5 165. Zatko was told that Twitter's Chief Privacy Officer had told the Board and
6 executives of the infringement a few years before, that the issue had been acknowledged,
7 but that nothing had been done. Zatko was told that the issue had also been raised with
8 engineering and leadership a few years before. Yet Twitter had done nothing.
9

10 166. Zatko learned that Defendants had misled the FTC concerning this very
11 issue. Years earlier, the FTC had asked Twitter questions about the training material it
12 had used to build its machine learning models. Truthful answers would reveal Twitter's
13 extensive violations of copyright and intellectual property rights. So, Twitter's strategy,
14 which executives explicitly acknowledged to Zatko as deceptive, was to point the FTC to
15 a small subset of models that did not use unlicensed materials and so would not expose
16 Twitter's violations. Zatko was told that Twitter hoped the FTC would draw the
17 incorrect conclusion that these models were representative.
18

19 167. Zatko also learned other ways in which Twitter had deliberately misled
20 regulators. According to Zatko's notes, Twitter was served with a subpoena in
21 connection with the investigation by DOJ Special Counsel Robert Mueller into, inter
22 alia, possible obstruction of justice by President Donald Trump and his associates.
23 Twitter initially responded that it had completed its production, but in 2017, discovered
24
25
26
27
28

1 that many of the documents that had been subpoenaed and which Twitter had thought
2 destroyed continued to exist in some of Twitter's vast unmanaged data pools.

3
4 168. Twitter only keeps track of and manages only about 20% of the datasets it
5 creates. This means that Twitter does not know what 80% of its data consists of, though
6 according to Zatko, searches have uncovered copious personally identifiable
7 information. For the same reason, Twitter cannot reliably delete Twitter users' data after
8 they delete their account. Twitter's senior executives and even its Board were made
9 aware of the problem, but Twitter did not remedy the problem.
10
11

12 169. The FTC Consent Order requires that Twitter responsibly maintain user
13 data. To ensure compliance, years before Zatko's hiring, the FTC asked Twitter whether
14 the data of users who cancelled their accounts had been deleted. Because Twitter does
15 not know what data it has, it would be lying if it said the data would be deleted. So,
16 instead, it misled the FTC, stating that the accounts were "deactivated," hoping the FTC
17 would not notice the distinction. Internally, Twitter had even calculated the financial
18 penalties it faced as a result of not being able to delete user information: \$3 million per
19 month plus 2% of revenues, running from the date of the violation, totaling hundreds of
20 millions of dollars in fines for just this violation.
21
22
23

24 **G. Defendants Make False Statements About mDAU**

25 170. In addition to Defendants' misrepresentations concerning Twitter's security
26 and privacy practices, during the Class Period Defendants systematically misrepresented
27
28

1 its “key metric,” monetizable daily active users (“mDAU”), by understating the number
2 of false and spam accounts included in mDAU, by falsely representing that mDAU
3 represented “monetizable” users, and by falsely claiming that mDAU was the best way
4 to measure engagement and user growth.
5

6 171. Until late 2018, Twitter told investors that its key metric was MAU, or
7 monthly active users, which is a widely accepted and standard metric among social
8 media and other digital product companies. But after three straight quarters of decreasing
9 MAUs, Twitter developed a new proprietary “key” metric—mDAU—that “grew”
10 continuously for ten straight quarter.
11
12

13 172. Rather than use more commonly-employed metrics, Twitter stated that it
14 “want[ed] to align our external stakeholders around one metric that reflects our goal of
15 delivering value to people on Twitter every day and monetizing that usage.” In its
16 disclosure replacing MAU with mDAU Twitter noted that “we believe that mDAU, and
17 its related growth, are the best ways to measure our success against our objectives and to
18 show the size of our audience and engagement going forward, so we will discontinue
19 disclosing MAU after the first quarter of 2019.”
20
21
22

23 173. During earnings calls, Twitter touted its mDAU growth alongside its
24 revenue numbers as the most important information for investors. Indeed, Twitter’s
25 CFO, Defendant Segal, told investors that “[w]hen we look at other markets, we’ve been
26
27
28

1 really pleased with the DAU growth, *which is the foundation of any revenue opportunity*
 2 *that we have.*”¹⁸

3
 4 *1. Almost a Third of Users Counted in mDAU Never Saw Any Ads*

5 174. When Twitter introduced its mDAU metric, it explained that “[o]ur mDAU
 6 are not comparable to current disclosures from other companies, many of whom share a
 7 more expansive metric *that includes people who are not seeing ads.*” The implication of
 8 Twitter’s statement is that mDAU only included people who saw ads.
 9

10 175. Twitter sued Musk to force him to complete his buyout of Twitter. Based on
 11 the discovery he received, Musk alleged that mDAU can be broken into four groups.
 12

13 176. The first of these groups consists of users who, despite being called
 14 monetizable, see no ads and generate no revenue. In Q1 2022, this group amounted to
 15 **29%** of the users counted in mDAU, or 65 million users.
 16

17 177. Worse, the proportion was increasing during 2021 and 2022. During a
 18 February 25, 2021, conference call, Dorsey announced a “goal of at least 315 million
 19 mDAU in the fourth quarter of 2023, which requires continued compounding growth at
 20 about 20% per year from the base of 152 million mDAU we reported in the fourth
 21 quarter of 2019.” Twitter did grow its mDAU, but as Musk alleges, more than half of the
 22 increase in mDAU in 2021 consisted of users who generated no revenues.
 23
 24

25
 26
 27 ¹⁸ Citi Global Technology Conference 2019, New York, New York (September 4,
 28 2019) (Ned Segal) at p. 6. After Twitter adopted its mDAU metric, it frequently
 interchangeably referred to mDAU and DAU.

1 178. Musk alleged that during 2021, the balance of users shifted sharply into
2 lower revenue categories. Musk's second group, which is 41% of mDAU, sees very few
3 ads and generates little revenue (estimated at roughly \$0.38 per user per month, or \$107
4 million per quarter in total, based on data provided by Twitter). The third group, which is
5 24% of mDAU, sees some ads and generates some revenue (roughly \$3.16 per user per
6 month, or \$512 million per quarter). The last group of power users, a mere 7% of
7 mDAU, views lots of ads and generates the most revenue per user (roughly \$11.55 per
8 user per month, or \$527 million per quarter). Less than 1% of the mDAU growth
9 reflected growth within this latter highly engaged group that was responsible for no
10 revenues.
11

12 179. Public disclosure of this stratification of mDAU to investors would show
13 that the number of monetizable Daily Active Users metric is not meaningful without
14 more information about the *users*.
15

16 2. *Twitter Knowingly Mislabeled Spam Accounts and Bots Within*
17 *mDAU*
18

19 180. One complication in calculating the mDAU metric is that Twitter's platform
20 contains a significant number of accounts that not only are not but cannot be monetized,
21 including false or spam accounts.
22

23 181. False or spam accounts can engage in a variety of behaviors that could lead
24 them to be counted as mDAU in the ordinary course, for example by logging into
25 Twitter and generating a high volume of tweets, retweets, and replies. But, because they
26
27
28

1 are generally not designed to engage with advertisements and ultimately buy products,
2 false and spam accounts are of no interest to advertisers and would be unlikely to ever
3 pay for subscription services. Additionally, these false or spam accounts often engage in
4 disruptive or abusive behavior—for example by mass replying to a user’s account or by
5 attempting to scam real users—that make the Twitter platform less appealing to its
6 legitimate users. Thus, such accounts do not present revenue opportunities. To the
7 contrary, they tend to diminish the experience of real users.

10 182. Understanding that fake and spam accounts would ordinarily be captured in
11 the mDAU metric, but do not represent actually monetizable users, Twitter purports to
12 exclude these accounts from its mDAU calculation. Twitter assured investors that it
13 “performed an internal review of a sample of accounts” and that “[a]fter we determine an
14 account is spam, malicious automation, or fake, we stop counting it in our mDAU, or
15 other related metrics. Purportedly based on this review, Twitter repeatedly stated in SEC
16 filings and elsewhere that spam and fake accounts “represented fewer than 5% of our
17 mDAU.” This less-than-5% figure has been unchanged since Twitter began disclosing
18 the mDAU metric in its 2018 10-K.

23 183. This was false. Twitter’s claim that fewer than 5% are fake or spam
24 accounts is purportedly the result of “the average of false or spam accounts in the
25 samples during each monthly analysis period during the quarter.” And Twitter states
26
27
28

1 that “[a]fter we determine an account is spam, malicious automation, or fake, we stop
2 counting it in our mDAU, or other related metrics.”

3
4 184. Yet as Musk alleged, the mDAU numbers that Twitter reported each
5 quarter, as Defendants knew, included accounts Twitter determined were fake *during the*
6 *quarter in which such accounts were counted in mDAU*. Thus, for example, if Twitter
7 determined on July 1, 2020, that a given user was a bot, that user would still be counted
8 in the mDAU metric Twitter disclosed for the quarter ending September 30, 2020.
9 Further, Twitter did not revise or restate mDAU figures to correct the inclusion of such
10 accounts in mDAU.
11
12

13 185. Twitter allegedly admitted to Musk that it does not remove spam accounts
14 from mDAU even after determining they are spam and suspending them for that reason.
15 Defendant Segal conceded during a July 1, 2022, call with Musk that the mDAU figures
16 it reports to investors includes these millions of accounts.
17
18

19 186. Twitter’s records indicate that nearly 5 million accounts suspended for
20 being spam during the first quarter of 2021 were included in the mDAU number reported
21 for that quarter, boosting the metric by 2.5%. Moreover, the number of suspended fake
22 or spam accounts included in mDAU increased sharply during the Class Period, reaching
23 13 million in the fourth quarter of 2021 (representing 6.2% of the 209.3 million mDAU
24 reported for that quarter) and 15 million in the first quarter of 2022 (6.9% of the 214.7
25 million mDAU reported for that quarter). Because they were suspended, these non-
26
27
28

1 revenue generating accounts were not “monetizable,” and it was misleading for Twitter
2 to include them as “*monetizable* Daily Active Users.”

3
4 187. Further, Twitter used a *de minimis* sample size of 100 user accounts to
5 assess the prevalence of spam and fake accounts for purposes of reaching the less-than-
6 5% result. This was not disclosed to the market until May 14, when Musk tweeted that
7 his “team will do a random sample of 100 followers of @twitter” to determine how
8 many were fake or spam accounts, and that “*I picked 100 as the sample size because that*
9 *is what Twitter uses to calculate <5% fake/spam/duplicate.*” Later that same day, Musk
10 tweeted: “Twitter legal just called to complain that I violated their NDA by revealing the
11 bot check sample size is 100! This actually happened.”

12
13
14
15 188. Twitter’s undisclosed use of a *de minimis* sample size was misleading in
16 light of the fact that Twitter had hundreds of millions of users, and in especially in
17 conjunction with Twitter’s decision not to exclude accounts suspended on the basis of
18 being fake or spam, and Twitter’s decision to disable its most effective anti-spam tool
19 (see Section IV.G.3, *infra*).

20
21
22 3. *Far More than 5% of mDAU and of Twitter’s User Base*
23 *Consisted of Fake and Spam Accounts.*

24 189. In addition to claiming that bots and spam were not included in mDAU,
25 Defendants claimed that such bots only accounted for about 5% of Twitter’s users.

26 190. For example, Defendants stated in a September 2021 article published on
27 Twitter’s official blog paraphrasing one of its senior executives that the number of bots
28

1 is “around 5% [] a number Twitter reports quarterly”. The tweet announcing the article
2 stated that “[b]elieve it or not, only around 5% of accounts on Twitter are bots.”

3
4 191. In truth, Twitter had no way of knowing how many bots there were on its
5 platform because it had made no attempt to count them. In early 2021, as a new
6 executive, Zatko asked the Head of Site Integrity (responsible for addressing platform
7 manipulation, including spam and “botnets,” which are automated “bot” accounts acting
8 in concert under the control of a person or group), what the underlying spam bot
9 numbers were. Their response was “we don’t really know.” The company could not even
10 provide an accurate upper bound on the total number of spam bots on the platform. The
11 site integrity team gave three reasons for this failure: (1) they did not know how to
12 measure; (2) they were overwhelmed by responding to frequent emergencies and could
13 not keep up with reacting to bots and other platform abuse; and, most troubling, (3)
14 senior management had no appetite to properly measure the prevalence of bot
15 accounts—because as Zatko later learned from a different sensitive source, they were
16 concerned that if accurate measurements ever became public, it would harm the image
17 and valuation of the company.
18

19
20 192. In addition, Zatko developed and presented to the Board of Directors a
21 sweeping, 3-year Board-supervised objective called “#Protect Initiative.” Elements of
22 the initiative would have assigned responsibility for properly measuring spam bot
23 prevalence. The entire senior leadership team and Board of Directors received and
24
25
26
27
28

1 approved Zatko's #Protect Initiative plan. If Twitter was already accurately measuring
2 and estimating spam bot prevalence on the platform, this issue would not have reached
3 the Board and been a specific part of Zatko's 2022 plans.
4

5 193. Bots were a low priority to Twitter. In or about the time of the Q3 2021
6 Board Risk Committee meeting, a Director asked why more progress had not been made
7 with respect to bots and related harmful content on the platform. Zatko remembers an
8 executive of the company admitting to Board members that the company had
9 "intentionally and knowingly deprioritized" platform health to focus on growing mDAU.
10
11 Afterwards, a different Twitter leader who had witnessed the exchange commented to
12 Zatko, in reference to this admission, "it is very strange what this company does not
13 share with board members, and then some of the statements that they do." Twitter had a
14 tool that effectively caught spam bots, but Defendants ultimately nixed it. "ROPO,"
15 which stands for "Read-Only Phone Only" (or "Read-Only Phone Ownership") is likely
16 Twitter's most volumetrically-effective mechanism for identifying and blocking spam
17 bots. If a script identifies an account as possibly spam and triggers ROPO, the account is
18 placed into a "Read Only" mode and is unable to post content to the platform. Twitter
19 sends a text message to the associated phone number, with a one-time code that the
20 recipient needs to manually enter to regain account access.
21
22
23
24
25
26
27
28

1 194. Shortly into Zatko's time at Twitter, a senior executive (with primary
2 responsibility for growing mDAU)¹⁹ proposed disabling ROPO worldwide, based on an
3 anecdote of a small number of unsolicited Direct Messages ("DMs," which are text
4 messages that users can send to each other) he had personally received from users
5 complaining they were incorrectly denied access by ROPO. The Lead of Site Integrity
6 told Zatko that executives responsible for growing mDAU had proposed disabling
7 ROPO several times before. The Site Integrity Lead pleaded with Zatko, as a senior
8 executive, to prevent the other executives from disabling ROPO. Research later
9 performed at Zatko's direction showed ROPO was effectively blocking more than 10-12
10 million bots each month with an exceptionally low rate (less than 1%) of false positives.
11

12 195. These efforts to prioritize increasing mDAU by declining to address fake
13 and spam accounts succeeded. According to documents produced in Musk's litigation
14 against Twitter, Twitter actively chose to *remove* ROPO in some of its most promising
15 new markets, including India (one of Twitter's largest markets), Nigeria, and Indonesia.
16 This demonstrates that Twitter knowingly allowed increased spam and fake accounts in
17 order to boost mDAU, contributing to the misleading impression of the health and
18 potential of Twitter's operations.
19
20
21
22
23
24
25
26

27
28 ¹⁹ Reportedly Defendant Beykpour.

1 196. Indeed, Musk has alleged that the percentage of Twitter accounts that are
2 bots is far greater than 5%—that, in fact, based on expert analysis of non-public data,
3 more than 10% of Twitter’s “users” are bots.
4

5 4. *mDAU Was Not a Key Metric Inside Twitter, But Was Used to*
6 *Cover Up Declining User Engagement*

7 197. Yet Twitter executives themselves did not rely on mDAU. Externally,
8 mDAU was the most important of only two “Key Metrics,” but that was not the case
9 inside the Company. Rather, Twitter executives relied on other metrics to measure user
10 engagement (implicitly recognizing the lesser reliability of mDAU) and thus to evaluate
11 the Company’s performance and revenue potential.
12
13

14 198. Twitter relies on advertising revenue, and advertisers use data about user
15 engagement to decide whether and how much to spend advertising on Twitter, and to
16 calculate the effectiveness of those ads. This provides an incentive for Twitter’s
17 executives to avoid counting spam bots as mDAU, which is publicly reported and thus
18 available to advertisers. If mDAU includes huge numbers of spam bots that do not click
19 through ads to buy products, then advertisers will conclude that their ads are less
20 effective, and might shift their ad spending away from Twitter to other platforms they
21 expect to be more effective.
22
23
24

25 199. Musk alleges that Defendants acknowledged internally that mDAU was not
26 the best indicator of Twitter’s success. Twitter’s executives and directors measure
27 engagement by calculating the total number of daily user active minutes (“UAM”) and
28

1 the total number of daily user active minutes per mDAU. Throughout 2021, those
2 figures were, at best, stagnant, and, at worst, declining. Twitter’s internal documents
3 reveal that these metrics declined, in large part, due to declines in engagement from
4 Twitter’s “most engaged” or “heaviest” users, i.e., the ones who drive a disproportionate
5 amount of Twitter’s revenues. On January 25, 2022, Twitter’s CEO, Parag Agrawal
6 wrote to Twitter’s head of data science—who was responsible for building Twitter’s
7 mDAU forecast model—and described the declining UAM figures as “concerning.”
8 Twitter’s head of data science responded that “the UAM decline is very concerning” and
9 that other measures of engagement had been “declining in concert with UAM per mDAU
10 for the engaged user segment for the last 18 months.” Despite knowledge of these stark
11 trends, Twitter continued to represent that mDAU was the “best way to measure”
12 engagement. This was a deliberate attempt by Twitter to convince investors that
13 engagement—which was critical to Twitter’s success—was increasing, while it knew
14 internally that engagement was down.

20 **H. A second whistleblower confirms Zatko’s claims**

21 200. On January 24, 2023, the *Washington Post* reported that a second Twitter
22 whistleblower had come forward concerning Twitter’s deficient cybersecurity and data
23 privacy practices. According to the article, “[t]he former employee has told members of
24 Congress and staff at the Federal Trade Commission that any Twitter engineer can
25 activate an internal program until recently called ‘GodMode’ and tweet from any
26
27
28

1 account today, three months after Musk's takeover." According to the former
2 employee's whistleblower complaint, which was confidentially filed with the FTC in
3 October 2022, and which was shared with the *Post* by a congressional staffer, Twitter
4 misled the public and investors about the steps it took to improve its privacy practices
5 after the 2020 security incident. "After the 2020 hack in which teenagers were able to
6 tweet as any account, Twitter publicly stated that the problems were fixed," the
7 complaint says. "However, the existence of GodMode is one more example that
8 Twitter's public statements to users and investors were false and/or misleading."
9
10

11
12 201. As the *Post* reported, this second whistleblower complaint alleged:

13 Though Twitter's then-leaders had said the number of people who had
14 access to such powerful tools had been cut in 2020, the new whistleblower
15 complaint says the GodMode code remains on the laptop of any engineer
16 who wants it. All they would have to do is change a line of the code from
17 FALSE to TRUE and run it from a production machine that they could reach
18 through an easily accessible communications protocol known as SSH.

19 202. Further, the *Post* reported: "They put in writing to the public and regulators
20 that they had closed all the loopholes," the new whistleblower said. "That's a lie."
21 Rather, "[t]hey removed this from one interface, but it still existed in other ways. They
22 just changed the lock on one of the many front doors."
23

24 203. The *Post* reported that it learned another former security engineer "that they
25 were aware of the problem and that improvements were somewhere in process when
26 they left the company late last year."
27
28

1 204. This latest whistleblower, echoing Zatko, reported to the Federal
2 government that they “ha[ve] a reasonable belief that the evidence in this disclosure
3 demonstrates legal violations by Twitter,” according to the *Post*.
4

5 **V. DEFENDANTS’ MISSTATEMENTS**

6 205. During the Class Period, Defendants made materially false and misleading
7 statements and omissions concerning Twitter’s security practices and compliance with
8 the FTC Consent Order, concerning mDAU and the prevalence of bots on Twitter, and
9 concerning Twitter’s use of intellectual property it did not own or license.
10

11 206. These misstatements were made in, *inter alia*, Twitter’s quarterly reports on
12 Form 10-Q and annual reports on Form 10-K, which were filed with the SEC.
13 Specifically, material misstatements were made in:
14
15

- 16 a. Twitter’s quarterly report on Form 10-Q for the quarter ended
17 June 30, 2020 (the “Q2 2020 10-Q”), signed by Defendants
18 Dorsey and Segal, and filed on August 3, 2020;
19
20 b. Twitter’s quarterly report on Form 10-Q for the quarter ended
21 September 30, 2020 (the “Q3 2020 10-Q”), signed by Defendants
22 Dorsey and Segal, and filed on October 30, 2020;
23
24 c. Twitter’s annual report on Form 10-K for the year ended
25 December 31, 2020 (the “2020 10-K”), signed by Defendants
26 Dorsey and Segal, and filed February 17, 2021;
27
28

- 1 d. Twitter's quarterly report on Form 10-Q for the quarter ended
2 March 30, 2021 (the "Q1 2021 10-Q"), signed by Defendants
3 Dorsey and Segal, and filed on April 30, 2021;
4
- 5 e. Twitter's quarterly report on Form 10-Q for the quarter ended
6 June 30, 2021 (the "Q2 2021 10-Q"), signed by Defendants
7 Dorsey and Segal, and filed on July 27, 2021;
8
- 9 f. Twitter's quarterly report on Form 10-Q for the quarter ended
10 September 30, 2021 (the "Q3 2021 10-Q"), signed by Defendants
11 Dorsey and Segal, and filed on October 27, 2021;
12
- 13 g. Twitter's annual report on Form 10-K for the year ended
14 December 31, 2021 (the "2021 10-K"), signed by Defendants
15 Agrawal, Dorsey, and Segal, and filed February 16, 2022;
16
- 17 h. Twitter's quarterly report on Form 10-Q for the quarter ended
18 March 30, 2022 (the "Q1 2022 10-Q"), signed by Defendants
19 Agrawal and Segal, and filed on May 2, 2022; and
20
- 21 i. Twitter's quarterly report on Form 10-Q for the quarter ended
22 June 30, 2022 (the "Q2 2022 10-Q"), signed by Defendants
23 Agrawal and Segal, and filed on July 26, 2022.
24
25

26 207. Together, the periodic reports set forth in the preceding paragraph are
27 referred to herein as the "Class Period Reports."
28

1 208. Attached to the Q2 2020 10-Q, Q3 2020 10-Q, 2020 10-K, Q1 2021 10-Q,
2 Q2 2021 10-Q, and Q3 2021 10-Q were certifications pursuant to the Sarbanes-Oxley
3 Act of 2002 (“SOX”) signed by Defendants Dorsey and Segal, representing that the
4 reports did not contain any untrue statement of a material fact and did not omit to state
5 any material fact necessary to make the statements made therein not misleading, and that
6 the financial information included in this report, fairly present in all material respects the
7 financial condition, results of operations and cash flows of the registrant as of, and for,
8 the periods presented in this report. Attached to the 2021 10-K, Q1 2022 10-Q, and Q2
9 2022 10-Q were SOX certifications signed by Defendants Agrawal and Segal, which
10 made the same representations.
11
12
13
14

15 209. In addition, on July 26, 2022, Twitter filed a definitive proxy statement on
16 Schedule 14A (the “Proxy Statement”). The Proxy Statement incorporated the 2021 10-
17 K and Q2 2022 10-Q by reference, and thus made the same materially false and
18 misleading statements as those filings, as set forth herein.
19

20 **A. Misstatements Implicating Compliance with the FTC Consent Order**

21 210. During the Class Period, Defendants made material misstatements
22 concerning (a) data privacy, (b) cybersecurity, and (c) compliance with the FTC Consent
23 Order.
24

25 211. These statements were false and misleading because: (a) Twitter gave
26 wildly overbroad access, in that around 50% of Twitter’s employees had access to
27
28

1 Twitter's source code and user data throughout the Class Period; (b) Twitter could not
 2 comply with users' requests concerning the use of their data because 80% of its data
 3 pools were unmanaged and contained user data Twitter would not know to delete; (c) as
 4 a result, Twitter repeatedly used data for purposes other than those users had granted; (d)
 5 Twitter's software was not secure, because around 50% of its servers were out of date,
 6 30% of its computers disabled auto update, and Twitter had no control over or
 7 knowledge of what software its employees installed; (e) Twitter did not log when its
 8 engineers accessed data, such that it could not catch instances of inappropriate access; (f)
 9 Twitter knowingly employed agents of foreign governments; and (g) Twitter tolerated
 10 manipulative campaigns conducted by at least one foreign government.
 11

12
 13
 14
 15 212. Additional reasons the statements are false and misleading are set out
 16 below.

17
 18 1. *Class Period Reports on Forms 10-K and 10-Q*

19 213. Twitter's Class Period reports on Forms 10-K and 10-Q stated:

20 Our products may contain errors or our security measures may be breached,
 21 resulting in the exposure of private information. Our products and services
 22 may be subject to attacks that degrade or deny the ability of people to access
 23 our products and services. These issues may result in the *perception* that our
 24 products and services are not secure, and people on Twitter and advertisers
 25 may curtail or stop using our products and services and our business and
 26 operating results could be harmed.

27 Our products and services involve the storage and transmission of people's
 28 and advertisers' information, and security incidents, including those caused
 by unintentional errors and those intentionally caused by third parties, may
 expose us to a risk of loss of this information, litigation, increased security

1 costs and potential liability. We and our third-party service providers
2 experience cyber-attacks of varying degrees on a regular basis. We expect to
3 incur significant costs in an effort to detect and prevent security breaches
4 and other security-related incidents, and we may face increased costs in the
5 event of an actual or perceived security breach or other security related
6 incident. In particular, the COVID-19 pandemic is increasing the
7 opportunities available to criminals, as more companies and individuals
8 work online, and as such, the risk of a cybersecurity incident potentially
9 occurring is increasing. ***We cannot provide assurances that our
preventative efforts will be successful.***

214. The Twitter's Class Period reports on Forms 10-K and 10-Q stated:

10 For example, in July 2020, we became aware of what we believe to be a
11 coordinated social engineering attack by people who successfully targeted
12 one or more of our employees with access to internal systems and tools. The
13 attackers used this access to target a small group of accounts (130) and to
14 gain control of a subset of these accounts and send Tweets from those
15 accounts and access non-public information relating to at least some of those
16 accounts. We are continuing to assess what other malicious activity the
17 attackers may have conducted and the extent to which non-public data
18 related to these accounts was compromised. ***We are also taking steps to
secure our systems while our investigations are ongoing.***

215. In addition to the reasons alleged at the beginning of this Subsection V.A.,
19 the statements in the previous paragraphs were false and misleading because Twitter was
20 not making any efforts to secure its systems. In fact, both the number and proportion of
21 its employees with plenary access to Twitter's source code and access to user data were
22 increasing. Further, Twitter already knew that its preventative efforts were not successful
23 because, among other things, in 2020, it had experienced 40 incidents, of which 20 were
24 breaches, and in one of which data of 200 million users had been exposed.

216. The Q2 2020 10-Q also stated:

1 While *we strive to comply with applicable privacy and data protection laws*
 2 *and regulations*, our privacy policies and other obligations we may have
 3 with respect to privacy and data protection, the failure or perceived failure to
 4 comply may result, and in some cases has resulted, in inquiries and other
 proceedings or actions against us by governments, regulators or others.

5 217. In addition to the reasons alleged at the beginning of this Subsection V.A.,
 6 these statements were false because Twitter knew that it did not comply with applicable
 7 privacy and data protection laws and regulations and, instead, concealed the violations
 8 by making affirmatively misleading statements to the FTC. Moreover, fact, both the
 9 number and proportion of its employees with plenary access to Twitter's source code and
 10 access to user data were increasing.
 11

13 2. *Statements in Presentations and Conferences*

14 218. On November 17, 2020, Defendant Dorsey testified to Congress. In a
 15 written statement, Dorsey stated:
 16

17 Protecting Privacy

18 In addition to the principles I have outlined to address content moderation
 19 issues in order to better serve consumers, it is also critical to protect the
 20 privacy of the people who use online services. We believe privacy is a
 21 fundamental human right, not a privilege. *We offer a range of ways for*
 22 *people to control their privacy experience on Twitter*, from offering
 23 pseudonymous accounts to letting people control who sees their Tweets to
 24 providing a wide array of granular privacy controls. *Our privacy efforts*
 25 *have enabled people around the world using Twitter to protect their own*
 26 *data*. That same philosophy guides how we work to protect the data people
 27 share with Twitter. *We empower the people who use our service to make*
 28 *informed decisions about the data they share with us*. We believe
 individuals should know, and have meaningful control over, what data is
 being collected about them, how it is used, and when it is shared. We believe
 that individuals should control the personal data that is shared with

1 companies and provide them with the tools to help them control their data.
 2 ***Through the account settings on Twitter, we give people the ability to***
 3 ***make a variety of choices about their data privacy, including limiting the***
 4 ***data we collect, determining whether they see interest-based advertising,***
 5 and controlling how we personalize their experience. In addition, we provide
 6 them with the ability to access information about advertisers that have
 7 included them in tailored audiences to serve them ads, demographic and
 8 interest data about their account from ad partners, and information Twitter
 9 has inferred about them.

10 219. In addition to the reasons alleged at the beginning of this Subsection V.A.,
 11 this statement gave the misleading impression that Twitter gave users control over the
 12 use of their data when, in fact, Twitter was unable to limit its access to purposes the user
 13 had consented to. Twitter did not enable its users “to protect their own data,” to have
 14 “meaningful control over[] what data is being collected about them, how it is used, and
 15 when it is shared,” or to “control the personal data that is shared with companies.”
 16 Twitter’s statements to users to the contrary were false.

17 220. During the February 25, 2021 analyst day presentation, Defendant Gadde
 18 stated:
 19

20 Finally, because we believe privacy is a fundamental human right, ***we will***
 21 ***continue to advocate for choice with respect to privacy and data protection.***
 22 We support regulatory proposals that enshrine thoughtful, innovative privacy
 23 protections into law. ***An internet structured around consumers meaningful***
 24 ***privacy choices*** will always be more open than one built around a business
 25 model that depends on accumulated stores of data for their own use.

26 221. Defendant Gadde also stated:

27 ***Our policies are built primarily around the promotion and protection of***
 28 ***three fundamental human rights, freedom of expression, safety, and***
privacy. These rights, among others, are enshrined in the Universal

1 Declaration of Human Rights, which is an international document adopted
 2 by the U.N. And numerous countries around the world. At times, these
 3 fundamental human rights can be in tension with each other. To address this
 4 tension, our rules attempt to establish an appropriate balance, *prioritizing
 safety above all others.*

5 222. In addition to the reasons alleged at the beginning of this Subsection V.A.,
 6 Defendant Gadde's statements gave the misleading impression that Twitter itself offered
 7 consumers meaningful privacy choices. In fact, Twitter literally could not ensure that its
 8 customers' data would only be used for purposes to which the customer had consented
 9 because it could not delete user data and did not know what 80% of its data was, though
 10 it knew it included customer data. Nor did Twitter prioritize users' safety. Instead, it
 11 consciously worked with oppressive regimes to help them crack down on dissidents.
 12

13 223. During the JP Morgan High Yield & Leveraged Finance Conference on
 14 March 2, 2021, Defendant Segal responded to an analyst question as follows:
 15

16 Q: Similar vein, different course perhaps, but there's been a lot of focus on
 17 content moderation at Twitter, how to promote healthy conversation. I think
 18 we've also talked about that last year. It's ongoing. But can you discuss
 19 some of the more recent steps the company has taken?
 20

21 A: So we're always working hard to make sure that people can trust the
 22 information they see and feel safe being a part of the conversation. That can
 23 mean new rules such as what we rolled out yesterday to make sure that
 24 people are not getting confused around vaccines for COVID-19. It means
 25 that *we're very careful around an election, whether it's in the United
 States or another part of the world* and making sure that civic integrity is
 26 respected and that people aren't confused about whether polling stations are
 27 open, whether they can vote by texting, whether somebody has been
 28 declared the victor or not in an election. We're labeling candidates. We are
 labeling, when appropriate, tweets to point people to the appropriate context.
 This is a piece of work that we'll be focused on forever that will constantly

1 be evolving based on the world around us. The example I provided around
 2 COVID-19 and vaccines, which is just from yesterday just gives you an
 3 example of how dynamic we must be as we consider the right policies for
 4 the environment in which we play. A year ago, when we were sitting at this
 5 conference, it was not clear we needed COVID-19 vaccines -- COVID-19
 6 policies, let alone COVID-19 vaccine policies.

7 224. In addition to the reasons alleged at the beginning of this Subsection V.A.,
 8 this statement gave the misleading impression that Twitter was able to make efforts to
 9 ensure civic integrity was respected around the world when, in fact, it did not have the
 10 language capacity to do so.

11 225. During the March 2, 2021 JP Morgan conference, Defendant Segal
 12 responded to another analyst question as follows
 13

14 A: True. So kind of tying that in, how do you think about content
 15 moderation? How does the company think about content moderation in the
 16 context of increased government and regulatory scrutiny? And it's not just
 17 Twitter, but similar platforms and even the context of Section 230. I think a
 18 lot of people like to bring up for different rules and different geographies
 19 that Twitter operates in.

20 Q: Sure. So the regulatory environment around us continues to be really
 21 dynamic as well, whether it's privacy-related issues in Europe or California
 22 or conversations around Section 230, which I'm sure will continue
 23 throughout this year. We feel like we have a really important and
 24 differentiated voice at the table in these conversations. Sometimes, it's just a
 25 small group of companies that end up talking in front of Congress about
 26 them, and we may have a different point of view where we believe strongly
 27 in transparency and choice. So let me double-click on those. ***Transparency***
 28 ***means we want people to know how we use their data. We want them to***
know how we make the decisions that we do, whether they're around
policies or how we surface tweets in their time line. We want them to have
choice on whether we use our -- their data or whether we use our
algorithms or not. An example on Twitter is if you open your Twitter app
 right now, and you go to the top right of your home timeline, you can toggle

1 back and forth between a reverse chronological time line and one where we
2 use our algorithm to surface the best tweets first. We first -- we've had that
3 feature in our app for years, but it was buried in your settings until about 1.5
4 years ago. *We were so proud to roll it out without really testing much*
5 *because we just felt it was the right thing to do: to give people choice and*
6 *to be transparent about where it was.* That really is top of mind to us as we
7 think about these conversations around the regulatory environment for
8 Internet companies. We don't want to see a regulatory construct that rewards
9 the largest companies who can hire content moderators. We want to see
10 companies be transparent in how they use data and how they use algorithms.
11 We want people to have choice in how the companies do those things. We
12 think that will ultimately end up serving everybody well around the Internet
13 conversation, whether its reviews on newsletters, reviews on products on an
14 e-commerce website or tweets.

15 226. In addition to the reasons alleged at the beginning of this Subsection V.A.,
16 the statements were false and misleading because users did not have a choice about how
17 Twitter used their data. Rather, Twitter would use the users' data for whatever it wished,
18 regardless of the user's consent. Further, Twitter did not want users to understand that
19 Twitter would not protect their privacy. The statement that Twitter rolled out a new
20 feature "because we just felt it was the right thing to do" was false; without a sandbox,
21 Twitter had no choice but to roll out features without substantial testing.

22 227. During a March 3, 2021 Morgan Stanley conference, Defendant Segal
23 responded to an analyst question about certain changes Apple was making to its privacy
24 policies as follows::

25 So first, it's too early for anyone in the industry, I think to approach IDFA
26 and convey any degree of certainty around how this plays out because the ad
27 platforms, the operating system providers, the advertisers and the people
28 who have the choice of how their data is used, all are going to have to act
and respond to these changes before we really know how it shakes out. So

1 this is going to take a while. Secondly, what gives us confidence and
 2 enthusiasm as we look ahead is we look at the unique signal that Twitter has,
 3 with a growing audience, with better formats and more relevance and the
 4 ability to better leverage that signal, much of which isn't tied to a device ID.
 We feel really good about our ability to leverage that combination.

5 *We also feel like we've built up a lot of trust with the people who use our*
 6 *service, whether it's around GDPR or CCPA. When we prompt people and*
 7 *ask them questions, we try to be really thoughtful and transparent and*
 8 *demonstrate the choices that they have. When we ask if we could show*
 9 *them personalized ads, we do the same thing.* We hope that, that trust that
 10 we've built up with people helps us as we look ahead, helping them
 11 understand the benefit of giving us the things that we need in order to give
 them a good experience, whether it's ads or tweets that they're seeing on
 Twitter.

12 228. On July 22, 2021 Twitter held an earnings call with analysts to discuss its
 13 financial results for the second quarter of 2021. During the call, Defendant Segal
 14 responded to an analyst question as follows:
 15

16 Q: Thanks. Two questions, please. Could you talk about what impact you
 17 would expect the Olympics to have on your outlook? What's embedded in
 18 there? I know from time to time you have called out events like World Cup
 19 contribution. So just talk about what the impact I guess of a crowd,
 Olympics is likely to be this year?

20 And then your commentary about IDFA or the Apple changes. It almost
 21 seems like your Alex more muted than what we hear or a little less uncertain
 22 than from other advertising platforms. Are there particular reasons why you
 23 think that the IDFA impact would be more certain would be clearer for you
 24 than it would be just give me it's maybe it's your advertiser base or the type
 of formats. Just any color on that would be helpful. Thanks a lot.

25 A: The second part of your question on ATT or IDFA. So far we're pleased
 26 with what we've seen, but it's too early to call a long-term trend. I point you
 27 to a few different things. *The first is we've worked really hard as long as*
 28 *the company has been around to build trust with the people who use our*
service. Hopefully, that means that when they're prompted from Twitter,

1 *then we give them a really clear explanation of what we're asking.*
 2 *Hopefully, that means they're more likely to accept the prompt from us*
 3 *than it they might be from others.*

4 229. The statements in the two paragraphs above were false and misleading
 5 because Twitter did not “work really hard” “to build trust”, nor had it “built up a lot of
 6 trust.” Instead, Twitter falsely told users it would respect their privacy, even though it
 7 was unable to.
 8

9 230. During a March 10, 2022 Morgan Stanley Conference, Defendant Agrawal
 10 responded to an analyst question as follows:
 11

12 Q: I want to talk about Europe a little bit and the unfortunate world the
 13 events around Russia and the Ukraine. Can you maybe just talk to us about
 14 how we should be thinking of potential impacts to the user growth, the
 15 advertising business or engagement on the platform as you sort of navigate
 16 through this uncertain time with Russia and Ukraine?

17 A: Yes. To talk about this event, I think it's important to take a step back. I
 18 think it's moments like this that sort of remind us, all of us who work on
 19 Twitter about like the importance of public conversation.

20 So our mission is to serve the public conversation. In this moment that
 21 reminds why public conversation is important in the world. Why Twitter is
 22 important in the world.

23 It's such a privilege to see our customers all around the world and how they
 24 use our service in this critical time. When things like this happen in the
 25 world, people show up on Twitter to find out what's happening. It gives us
 26 this opportunity to showcase the value of Twitter to all of these people. But
 27 it also has us feel this immense responsibility, right?

28 So -- and I think it reinforces for me personally sort of the approach we've
 taken over the years around improving the health of the public conversation
 to be really proactive and principled around that.

1 It gives me pride in our team because back in 2017, on the ad side, we off-
 2 boarded RT and Sputnik. In 2019, we banned all ads from state-affiliated
 3 media organization. Back in 2020, we started labeling and de-amplifying all
 state-affiliated media entities.

4 *So -- and over the years, we've been very, very transparent about any*
 5 *attempt that we've seen from state actors to manipulate the conversation*
 6 *on Twitter, right? And we've shared those transparently. We've been*
 7 *active in detecting them.*

8 So really, we've been doing work proactively to be prepared for this
 9 moment. And even in the last two weeks, our teams have done a lot of
 amazing work, right?

10 231. In addition to the reasons alleged at the beginning of this Subsection V.A.,
 11 this statement was false and misleading because even as Agrawal spoke, Twitter was
 12 tolerating and concealing a brutal influence campaign from the Chinar Corp that
 13 included targeting journalists for violence. Twitter deliberately did so to curry favor with
 14 India's ruling party.

17 3. *Official Twitter Blog posts*

18 a. September 24, 2020 blog post

19 232. On September 24, 2020, Defendant Agrawal and Twitter's Chief Privacy
 20 Officer ("CPO") Damien Kieran issued a post on Twitter's official blog, which Twitter
 21 maintains on its website.²⁰ The post, entitled "Our continued work to keep Twitter
 22 secure," stated that:

23
 24
 25
 26
 27 ²⁰ See [https://blog.twitter.com/en_us/topics/company/2020/our-continued-work-to-](https://blog.twitter.com/en_us/topics/company/2020/our-continued-work-to-keep-twitter-secure)
 28 [keep-twitter-secure](https://blog.twitter.com/en_us/topics/company/2020/our-continued-work-to-keep-twitter-secure).

1 We are constantly working to balance how we build products and provide
 2 support to people who use Twitter while ensuring the security and privacy of
 3 people who use our service. *That means access is limited and is only*
 4 *granted for valid business reasons (i.e., ensuring an account holder can*
get support if they are locked out of their account).

5 * * * * *

6 *To further secure our internal tools from potential misuse, we have been*
 7 *strengthening the rigorous checks that team members with access must*
 8 *undergo.* This also helps reduce the potential for an unauthorized person to
 9 get access to our systems. *We have strict principles around who is allowed*
 10 *access to which tools and at what time, and require specific justifications*
for customer data to be accessed.

11 * * * * *

12 Similar to how we proactively detect and alert you of suspicious behavior on
 13 your account to help you keep it secure, we have internal detection and
 14 monitoring tools that help alert us of unusual behavior or possible
 15 unauthorized attempts to access our internal tools. *These tools are*
 16 *constantly being improved, even since the July incident, to include things*
 17 *like expanding our detection and response efforts to include suspicious*
authentication and access activity.

18 233. In addition to the reasons alleged at the beginning of this Subsection V.A.,
 19 the statement was false and misleading because: (a) almost half of Twitter's employees
 20 could access accounts for any reason; (b) Twitter had no way of logging its employees'
 21 attempts to access accounts so it would not even know in retrospect who had accessed
 22 customer data; and (c) Twitter could not even limit its access to data to those uses
 23 customers had consented to. Further, Twitter did not perform meaningful vetting for
 24 employees with privileged access, nor were team members with access to production
 25 systems and data evaluated differently from other employees. For the vast majority of
 26
 27
 28

1 methods that staff and contractors used to access sensitive data, including user data, there
2 were no time-based limits on access; rather, such limits applied only to a small subset of
3 tools.
4

5 234. It further stated:

6 In addition to requiring Security and Privacy & Data Protection training for
7 all newly hired Twitter employees, we introduced new courses and increased
8 the frequency and availability of existing courses for all employees. For
9 example, we introduced two new mandatory training sessions for people
10 who have access to non-public information. These trainings make clear the
11 dos and don'ts when accessing this information and ensure employees
12 understand how to protect themselves when they are online so they can
13 better avoid becoming phishing targets for attackers. In addition to existing
14 security training courses, we've also enhanced training content on secure
coding, threat modeling, privacy impact assessments, and privacy by
default.

15 235. In addition to the reasons alleged at the beginning of this Subsection V.A.,
16 this statement was false and misleading because Twitter did not have "enhanced training
17 content on secure coding, threat modeling, privacy impact assessments, and privacy by
18 design so privacy is integrated into everything we design and build by default." Twitter
19 neither followed an industry-appropriate SDLC nor had one been rolled out across
20 engineering and existing projects and programs. If and when the InfoSec or Privacy
21 teams learned about a project, security and privacy reviews often had to be forced into
22 projects. It was further noted that very few of the products submitted for security and/or
23 privacy review included threat modeling on how the products could be abused by bad
24
25
26
27
28

1 actors. The omission of threat modeling indicated that engineers had not considered the
2 question of vulnerabilities.

3
4 236. It further stated:

5 Our teams have also been investing in additional penetration testing and
6 scenario planning to help secure Twitter from a range of possible threats,
7 including in the context of the upcoming 2020 US elections. Specifically,
8 over a five month period from March 1 to August 1, Twitter's cross-
9 functional elections team conducted tabletop exercises internally on specific
10 election scenarios. Some of the topics included: hacks and other security
11 incidents, leaks of hacked materials, platform manipulation activity, foreign
12 interference, coordinated online voter suppression campaigns, and the post
13 election day period.

14 237. In addition to the reasons alleged at the beginning of this Subsection V.A.,
15 this statement was false and misleading because Twitter did not have "teams [that] have
16 also been investing in additional penetration testing and scenario planning," as Twitter
17 had neither an internal red team nor a third party that reported to Zatko, the then-Security
18 Lead, and was engaged in meaningful internal penetration testing within the InfoSec
19 organization.

20 238. It further stated:

21 Finally, we continue to invest in and scale the processes in place to review
22 products for security and privacy concerns before they launch. If a project
23 could have significant privacy impacts, we conduct a detailed impact
24 assessment to make sure we're taking appropriate measures before we
25 launch it. We've significantly increased the number of privacy reviews and
26 impact assessments the past few years. Specifically, in 2018, we did about
27 100 privacy reviews; in 2019, we did almost 500 privacy reviews; and in the
28 first 6 months of 2020, we have completed more than 300 privacy reviews.

239. In addition to the reasons alleged at the beginning of this Subsection V.A., this statement was misleading because until 2021 Twitter did not employ trained Privacy Engineers. Instead, Twitter relied on regular engineers to implement privacy measures without the benefit of guidance from senior Privacy Engineering leadership or people with appropriate domain expertise.

a. November 26, 2020 blog post

240. On November 26, 2022, Twitter issued a blog post co-authored by Katy Minshall, then the Head of Government, Public Policy and Philanthropy for Twitter UK, which stated:

Platforms like Twitter have taken a number of important steps to confront this problem, for example - having a dedicated site integrity team and continuous investment in technology to detect, understand and neutralize these campaigns as quickly and robustly as possible - but technology companies can't do it alone.

* * * * *

Second, it raises general awareness and increases understanding more widely of the scale and nature of the challenges impacting the integrity of public conversation online. This is why *in 2018, Twitter committed to disclose publicly, any state-backed information operations that were reliably identified on the service, and to make the full datasets of those operations available for investigation and analysis. Since this first release over two years ago, Twitter has now disclosed over 35 separate state-backed information operations designed to nefariously shape and manipulate public opinion online.* Independent analysis of this activity by researchers is a key step toward promoting shared understanding of these threats and to help develop a holistic strategy for addressing them.

And third, making this data available keeps platforms like Twitter accountable for their own response to these challenges. The nature of

1 conversations taking place on Twitter is well-documented and, critically,
 2 members of the public, governments, and researchers can bring their
 3 expertise to bear to develop solutions for a range of online harms. However,
 4 as Twitter's CEO, Jack Dorsey has said, there is much more to do when it
 5 comes to transparency; and *the team within Twitter who work with
 researchers are part of that, constantly looking for opportunities to provide
 new data while balancing privacy considerations.*

6 241. In addition to the reasons alleged at the beginning of this Subsection V.A.,
 7
 8 the statements were misleading because Twitter concealed the virulent foreign influence
 9 operation run by the Chinar Corp.

10 a. May 25, 2022 blog post
 11

12 242. On May 25, 2022, CPO Damien Kieran issued a post on Twitter's blog.²¹
 13 The post, entitled "FTC settlement: Our commitment to protecting your privacy and
 14 security," stated that
 15

16 On May 25, 2022, Twitter reached a settlement with the Federal Trade
 17 Commission (FTC) regarding a privacy incident disclosed in 2019 when
 18 some email addresses and phone numbers provided for account security
 19 purposes may have been inadvertently used for advertising. *This issue was
 addressed as of September 17, 2019*, and today we want to reiterate the
 20 work we'll continue to do to protect the privacy and security of the people
 21 who use Twitter.

22 Keeping data secure and respecting privacy is something we take extremely
 23 seriously, and we have cooperated with the FTC every step of the way. In
 24 reaching this settlement, we have paid a \$150M USD penalty, and we have
 25 aligned with the agency on operational updates and program enhancements
 26 to ensure that people's personal data remains secure and their privacy
 27 protected.

28 ²¹ See https://blog.twitter.com/en_us/topics/company/2022/ftc-settlement-twitter.

1 243. In addition to the reasons alleged at the beginning of this Subsection V.A.,
 2 this was false and misleading because: (i) Twitter had not, as of September 17, 2019,
 3 ended its practice of using email addresses and phone numbers provided for account
 4 security purposes for advertising; (ii) Twitter did not take “[k]eeping data secure and
 5 respecting privacy . . . extremely seriously.”
 6

7
 8 4. *Agrawal interview with Wired magazine*

9 244. Agrawal told *Wired* for a September 28, 2020, article that “[t]he amount of
 10 access, the amount of trust granted to individuals with access to these tools, is
 11 substantially lower today.”
 12

13 245. In addition to the reasons alleged at the beginning of this Subsection V.A.,
 14 the statement gave the misleading impression that Twitter had addressed the problem
 15 that led to the July 2020 hack though, in fact, Twitter gave plenary access to almost half
 16 of its employees.
 17

18
 19 **B. Misstatements Concerning mDAU**

20 246. As set out in this Subsection V.B., during the Class Period, Defendants
 21 made false and misleading statements (1) concerning the manner in which Twitter
 22 calculated mDAU, and (2) claiming that mDAU was the most important metric to
 23 evaluating user engagement, user growth, and Twitter’s revenue potential.
 24

25 247. These statements were all false and misleading for the same reasons: (a)
 26 when Twitter introduced mDAU, it claimed that “[o]ur mDAU are not comparable to
 27
 28

current disclosures from other companies, many of whom share a more expansive metric that includes people who are not seeing ads”, but nearly a third of Twitter users counted in mDAU never saw ads and never earned Twitter any money; (b) the prevalence of such accounts was increasing; (c) Twitter internally relied on metrics other than mDAU to measure its success and the size of its audience and engagement; (d) these other metrics of user engagement, especially UAM, more closely tracked revenue and were declining (by contrast to Twitter’s reported mDAU growth); (e) 10% of Twitter’s users were bots or spam; and (f) Twitter “intentionally deprioritized” removal of spam and fake accounts.

248. Additional reasons particular statements were false or misleading are alleged below following each statement.

1. Class Period Reports on Forms 10-K and 10-Q

249. The Q2 2020 10-Q made a series of false and misleading statements and omissions concerning Twitter’s mDAU metric and the amount of spam and bots included in mDAU. Materially identical statements were also made in rest of Twitter’s Class Period Reports.

250. Twitter’s Class Period reports on Forms 10-K and 10-Q stated that:

We believe that mDAU, and its related growth, is the best way to measure our success against our objectives and to show the size of our audience and engagement.

251. The Q2 2020 10-Q and Q3 2020 10-Q also stated that:

1 For example, *we believe that mDAU, and its related growth, are the best*
 2 *ways to measure our success against our objectives and to show the size of*
 3 *our audience and engagement going forward, so we discontinued*
 4 *disclosing monthly active usage after the first quarter of 2019.*

5 252. Twitter's Class Period reports on Forms 10-K and 10-Q stated that: "***Our***
 6 ***advertising revenue growth is primarily driven by increases in mDAU,*** increases in ad
 7 pricing or number of ads shown and increases in our clickthrough rate."

8 253. In addition to the reasons alleged at the beginning of this Subsection V.B.,
 9 the statements in the foregoing three paragraphs are false and misleading because: (a)
 10 Twitter used UAM to measure user engagement, not mDAU; (b) a large and growing
 11 proportion of Twitter's mDAU accounts consisted of users from whom Twitter never
 12 earned any revenues.
 13

14 254. Twitter's Class Period reports on Form 10-Q stated the following (and the
 15 Class Period Reports on Form 10-K said the same thing, while replacing "Annual
 16 Report" for "Quarterly Report"):
 17

18 The numbers of mDAU presented in this Quarterly Report on Form 10-Q are
 19 based on internal company data. While ***these numbers are based on what***
 20 ***we believe to be reasonable estimates for the applicable period of***
 21 ***measurement,*** there are inherent challenges in measuring usage and
 22 engagement across our large number of total accounts around the world.
 23

24 255. The Q2 2020 10-Q stated the following (and Twitter's other Class Period
 25 reports on Forms 10-Q and 10-K contained materially identical statements, each
 26 referencing the most recently ended quarter):
 27
 28

1 *We have performed an internal review of a sample of accounts and*
 2 *estimate that the average of false or spam accounts during the second*
 3 *quarter of 2020 represented fewer than 5% of our mDAU during the*
 4 *quarter.*

5 256. The Q2 2020 10-Q stated the following (and Twitter's other Class Period
 6 reports on Forms 10-Q and 10-K contained materially identical statements, each
 7 referencing the most recently ended quarter):

8 *We estimate that the average of false or spam accounts during the first*
 9 *quarter of 2020 continued to represent fewer than 5% of our mDAU*
 10 *during the quarter.*

11 257. Twitter's Class Period reports on Forms 10-K and 10-Q stated that:

12 *We are continually seeking to improve our ability to estimate the total*
 13 *number of spam accounts and eliminate them from the calculation of our*
 14 *mDAU*, and have made improvements in our spam detection capabilities that
 15 have resulted in the suspension of a large number of spam, malicious
 16 automation, and fake accounts.

17 258. Twitter's Class Period reports on Forms 10-K and 10-Q stated that:

18 *We are continually seeking to improve our ability to estimate the total*
 19 *number of spam accounts and eliminate them from the calculation of our*
 20 *mDAU*, but we otherwise treat multiple accounts held by a single person or
 21 organization as multiple accounts for purposes of calculating our mDAU
 22 because we permit people and organizations to have more than one account.

23 259. In addition to the reasons alleged at the beginning of this Subsection V.B.,
 24 the statements in the foregoing five paragraphs are false and misleading because: (a)
 25 Twitter included accounts already identified as spam or bot in its count of mDAU; (b)
 26 almost a third of mDAU were not monetized; and (c) the method Twitter employed to
 27 calculate mDAU was completely unreliable.
 28

1 260. Twitter's Class Period reports on Forms 10-K and 10-Q stated that:

2 *After we determine an account is spam, malicious automation, or fake, we*
 3 *stop counting it in our mDAU, or other related metrics.*

4 261. In addition to the reasons alleged at the beginning of this Subsection V.B.,
 5 the foregoing statement was false and misleading because Twitter reported mDAU that
 6 included a material number of accounts that it had already determined to be fake or spam
 7 accounts and had suspended on that basis.
 8

9
 10 2. *Conference Calls and Presentations*

11 262. During the August 11, 2020 Oppenheimer conference, Segal, in response to
 12 a question about providing more clarity about Twitter's number of users, stated:
 13

14 So about a year-and-a-half ago, we transitioned to really just talk about
 15 monetizable daily active usage, and the reason we did that is that's what
 16 we've been tracking internally for a long time as the best way to measure
 17 our success in getting people to use Twitter as a daily part of their lives.

18 263. On February 25, 2021, Twitter convened its "2021 Analyst Day" and held a
 19 conference call with analysts. During the call, Kayvon Beykpour, told analysts:
 20 "[u]ltimately, we measure our long term success through our ability to grow monetizable
 21 daily active usage (mDAU)," and that while "there are a variety of metrics that help us
 22 gauge whether our product solutions are working, [] in [the] aggregate the best way to
 23 measure our success is mDAU."
 24

25 264. In addition to the reasons alleged at the beginning of this Subsection V.B.,
 26 the statements' in the foregoing two paragraphs were false and misleading because: (a)
 27
 28

1 Twitter did not primarily rely on mDAU to gauge its success; and (b) a large and
2 growing proportion of Twitter's mDAU accounts consisted of users from whom Twitter
3 never earned any revenues.
4

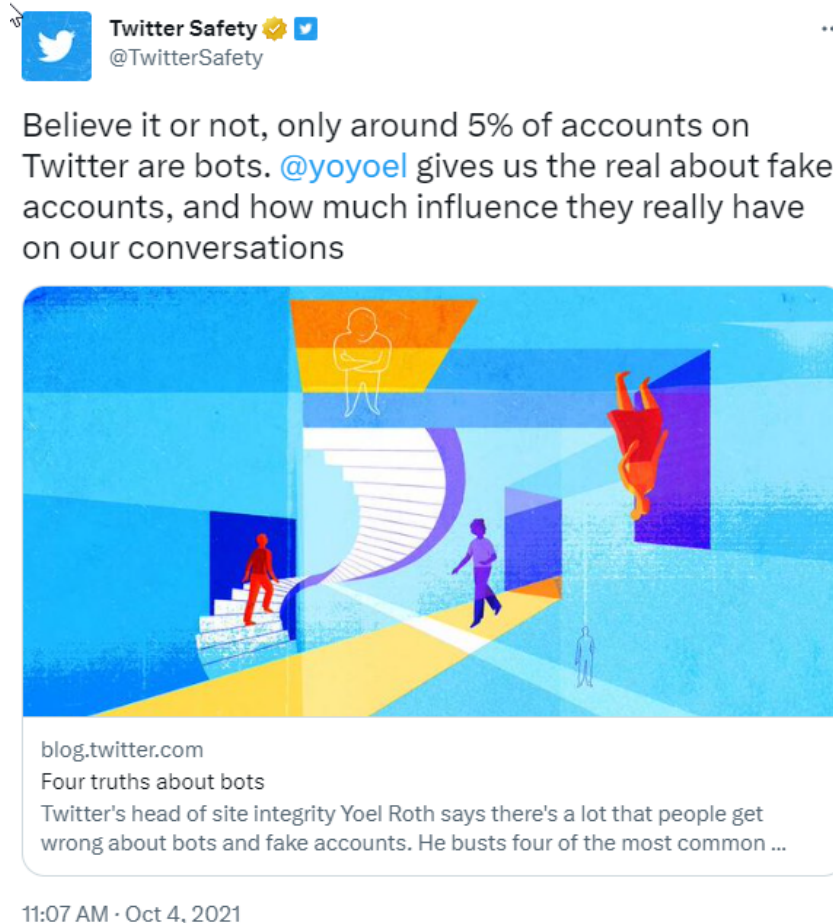
5 265. During the call, Beykpour also stated:

6 Today, we want to give you a bit more insight into that strategy. Our
7 strategy falls into three key areas, what we call Health, Interests and
8 Conversations. Let's talk about each. We believe it is essential for public
9 conversation to be healthy. If people don't feel that their conversations are
10 safe from abuse and harassment, we know they won't feel comfortable
11 participating in the first place. ***And if content on the platform is rife with
spam or misleading information, people won't trust the integrity of the
platform. Mitigating these risks is critical for us to create the best
experience for our customers, and ultimately critical in supporting our
growth.*** Ensuring a healthy public conversation is also essential for our
12 advertisers, who want to ensure that their brand and activity are not active
13 alongside harassment, vitriol and misleading information.
14

15 266. In addition to the reasons alleged at the beginning of this Subsection V.B.,
16 Beykpour's statements were false because Twitter had intentionally deprioritized bot
17 removal.
18

19 3. *September 21, 2021 Tweet*
20

21 267. On September 21, 2021, Twitter tweeted that "only around 5% of accounts
22 on Twitter are bots":
23
24
25
26
27
28



268. The article referenced in the tweet stated that “the number of bots, [is] around 5%, a number Twitter reports quarterly”.

269. In addition to the reasons alleged at the beginning of this Subsection V.B., the statements in the previous two paragraphs were false and misleading because Twitter had no idea how many of its users were bots because it had never tried to measure the proportion, let alone report it quarterly.

1 4. *Defendant Agrawal’s False and Misleading Tweets in May*
 2 *2022*

3 270. On May 16, 2022, Defendant Agrawal issued a series of related tweets
 4 (called a “tweet thread”) that included the following tweets:

5 a. “First, let me state the obvious: spam harms the experience for
 6 real people on Twitter, and therefore can harm our business. *As*
 7 *such, we are strongly incentivized to detect and remove as much*
 8 *spam as we possibly can, every single day.* Anyone who suggests
 9 otherwise is just wrong.”

10 b. “*Our team updates our systems and rules constantly to remove*
 11 *as much spam as possible*, without inadvertently suspending real
 12 people or adding unnecessary friction for real people when they
 13 use Twitter: none of us want to solve a captcha ever time we use
 14 Twitter.”

15 271. In addition to the reasons alleged at the beginning of this Subsection V.B.,
 16 these statements were false and misleading because as Defendant Agrawal disclosed to
 17 Twitter’s Board, Twitter had intentionally deprioritized spam and bot identification and
 18 removal
 19

20 **C. Misstatements Implicating Twitter’s Use of Stolen Intellectual Property**

21 272. The Q2 2020 10-Q, Q3 2020 10-Q, and 2020 10-K stated:
 22
 23
 24

1 Companies in the internet, technology and media industries are subject to
2 litigation based on allegations of infringement, misappropriation or other
3 violations of intellectual property rights. Many companies in these
4 industries, including many of our competitors, have substantially larger
5 patent and intellectual property portfolios than we do, which could make us
6 a target for litigation as we may not be able to assert counterclaims against
7 parties that sue us for patent, or other intellectual property infringement. In
8 addition, various “non-practicing entities” that own patents and other
9 intellectual property rights often attempt to assert claims in order to extract
10 value from technology companies. From time to time we receive claims
11 from third parties which allege that we have infringed upon their intellectual
12 property rights. Further, from time to time we may introduce new products,
13 product features and services, including in areas where we currently do not
14 have an offering, which could increase our exposure to patent and other
15 intellectual property claims from competitors and non-practicing entities. In
16 addition, although our standard terms and conditions for our Promoted
17 Products and public APIs do not provide advertisers and platform partners
18 with indemnification for intellectual property claims against them, some of
19 our agreements with advertisers, content partners, platform partners and data
20 partners require us to indemnify them for certain intellectual property claims
21 against them, which could require us to incur considerable costs in
22 defending such claims, and may require us to pay significant damages in the
23 event of an adverse ruling. Such advertisers, content partners, platform
24 partners and data partners may also discontinue use of our products, services
25 and technologies as a result of injunctions or otherwise, which could result
26 in loss of revenue and adversely impact our business.

27 We presently are involved in a number of intellectual property lawsuits, and
28 as we face increasing competition and develop new products, we expect the
number of patent and other intellectual property claims against us may grow.
There may be intellectual property or other rights held by others, including
issued or pending patents, that cover significant aspects of our products and
services, and **we cannot be sure that we are not infringing or violating, and
have not infringed or violated, any third-party intellectual property rights
or that we will not be held to have done so or be accused of doing so in the
future.** Any claim or litigation alleging that we have infringed or otherwise
violated intellectual property or other rights of third parties, with or without
merit, and whether or not settled out of court or determined in our favor,
could be time-consuming and costly to address and resolve, and could divert
the time and attention of our management and technical personnel. Some of

our competitors have substantially greater resources than we do and are able to sustain the costs of complex intellectual property litigation to a greater degree and for longer periods of time than we could. The outcome of any litigation is inherently uncertain, and there can be no assurances that favorable final outcomes will be obtained in all cases. In addition, plaintiffs may seek, and we may become subject to, preliminary or provisional rulings in the course of any such litigation, including potential preliminary injunctions requiring us to cease some or all of our operations. We may decide to settle such lawsuits and disputes on terms that are unfavorable to us. Similarly, if any litigation to which we are a party is resolved adversely, we may be subject to an unfavorable judgment that may not be reversed upon appeal. The terms of such a settlement or judgment may require us to cease some or all of our operations or pay substantial amounts to the other party. In addition, we may have to seek a license to continue practices found to be in violation of a third-party's rights. If we are required, or choose to enter into royalty or licensing arrangements, such arrangements may not be available on reasonable terms, or at all, and may significantly increase our operating costs and expenses. As a result, we may also be required to develop or procure alternative non-infringing technology, which could require significant effort and expense or discontinue use of the technology. An unfavorable resolution of the disputes and litigation referred to above would adversely impact our business, financial condition and operating results.²²

273. This statement was false and misleading because Twitter senior leadership have known for years that the company has never held proper licenses to the data sets and/or software used to build some of the key Machine Learning models used to run the service. Further, in response to questions about the training material used to build Twitter's machine learning models, Twitter misled the FTC in order not to reveal that it had committed extensive violations of copyrights and intellectual property rights of other

²² Twitter's subsequent Class Period Reports contained a statement that was identical other than removing "we expect" from the first sentence of the second quoted paragraph.

1 persons and entities. Further, Zatko was told by a senior privacy officer at Twitter that
2 in early 2022, Twitter planned to similarly deceive Irish and French regulators. Thus,
3 Defendants knew that Twitter's key products *did* violate others' intellectual property
4 rights. Moreover, warning of a large number of boilerplate risk factors generally
5 applicable to all technology companies gave investors the misleading impression that
6 Twitter's intellectual property was at no greater risk than that of other technology
7 companies when in fact, Twitter's key products were built on misappropriated
8 intellectual property.
9
10
11

12 **VI. LOSS CAUSATION**

13 274. Defendants' false statements artificially inflated the price of Twitter's stock.
14 Beginning in February 2022, a series of revelations dissipated the artificial inflation.
15

16 275. Twitter's early history was marred by frequent outages, so much so that the
17 image Twitter displayed when it was down became an internet meme.
18

19 276. Yet over the years, Twitter outages became less frequent. Twitter did not
20 experience any major outages in 2021. And when its social media rivals went down in
21 October 2021, Twitter gloated, tweeting "Hello literally everyone" during the outage to
22 highlight that users flocked to Twitter to complain of Facebook's outage.
23

24 277. So it came as a surprise when, on February 11, 2022, Twitter experienced a
25 major outage. Over 40,000 customers spread across the U.S., Canada, the UK, France,
26 Mexico and India took the time to complain to third-party website downdetector.com
27
28

1 that they had lost access to their Twitter account. There were likely millions or tens of
2 millions who suffered outages but did not make the effort to complain. This first incident
3 marked the start of a series of embarrassing outages that took place all through 2022.
4

5 278. In response to this news, the price of Twitter's common stock fell 3.34%, or
6 \$1.24, from a closing price of \$37.08 on February 10, 2022, to close at \$35.84 on
7 February 11, 2022.
8

9 279. On April 14, 2022, Musk made an offer to buy Twitter, which Twitter's
10 Board accepted on April 25. Three days later, Twitter restated its mDAU for Q4 2020
11 and each quarter of 2021, acknowledging that it had double counted millions of users.
12

13 280. Musk quickly requested that Twitter explain to him how it counted bots and
14 spam accounts in mDAU, which it attempted to do on a May 6, 2022, call with Musk.
15

16 281. On Monday May 9, 2022, Musk texted the investment banker who was
17 advising him on the Twitter acquisition:
18

19 An extremely fundamental due diligence item is understanding exactly how
20 Twitter confirms that 95% of their daily active users are both real people and not
21 double-counted. They couldn't answer that on Friday, which is insane... To be
22 super clear, this deal moves forward if it passes due diligence, but obviously not if
there are massive gaping issues.

23 282. Musk made several more requests that Twitter explain how it identified
24 such accounts and justify its count.
25
26
27
28

1 283. Unsatisfied, on May 13, 2022, before the market opened, Musk tweeted:
2 “Twitter deal temporarily on hold pending details supporting calculation that spam/fake
3 accounts do indeed represent less than 5% of users.”
4

5 284. Musk continued to tweet about this issue during the trading day on May 13,
6 including tweets suggesting that Twitter’s public representations concerning fake or
7 spam accounts (and thus regarding mDAU) were false.
8

9 285. In response to this news, the price of Twitter’s common stock fell 9.67%, or
10 \$4.36, from a closing price of \$45.08 on May 12, 2022, to close at \$40.72 on May 13,
11 2022.
12

13 286. On the weekend of May 14 and 15, 2022, Musk continued to tweet about
14 the prevalence of fake or spam accounts on Twitter. On May 14, Musk tweeted that his
15 “team will do a random sample of 100 followers of @twitter” to determine how many
16 were fake or spam accounts, and that “I picked 100 as the sample size because that is
17 what Twitter uses to calculate <5% fake/spam/duplicate.” Later that same day, Musk
18 tweeted: “Twitter legal just called to complain that I violated their NDA by revealing the
19 bot check sample size is 100! This actually happened.” On May 15 he said in two tweets
20 that “I have yet to see *any* analysis that has fake/spam/duplicates at 5%”. Further,
21 during the trading day on May 16, 2022, in response to tweets by Defendant Agrawal
22 concerning the prevalence of fake or spam accounts, Musk asked on Twitter “So how do
23
24
25
26
27
28

1 advertisers know what they're getting for their money? This is fundamental to the
2 financial health of Twitter.”

3
4 287. In response to this news, the price of Twitter's common stock fell 8.18%, or
5 \$3.33, from a closing price of \$40.72 on May 13, 2022, to close at \$37.39 on the next
6 trading day, May 16, 2022.

7
8 288. On July 7, 2022, after close of trading, the *Washington Post* reported that
9 Musk's agreement to acquire Twitter was “in peril.” The *Post* reported, based on three
10 anonymous sources with knowledge, that Musk and his team concluded that they could
11 not verify Twitter's claims regarding fake and spam accounts, were prepared to make “a
12 change in direction,” and had “stopped engaging in certain discussions around funding”
13 for the acquisition.
14

15
16 289. In response to this news, the price of Twitter's common stock fell 5.1%, or
17 \$1.98, from a closing price of \$38.79 on July 7, 2022, to close at \$36.81 on July 8, 2022.
18

19 290. After the market closed on July 8, 2022, Twitter publicly filed with the SEC
20 a letter it received from Musk's counsel stating that Musk was terminating the merger
21 agreement “because Twitter is in material breach of multiple provisions of that
22 Agreement, appears to have made false and misleading representations upon which Mr.
23 Musk relied when entering into the Merger Agreement, and is likely to suffer a Company
24
25
26
27
28

1 Material Adverse Effect (as that term is defined in the Merger Agreement).”²³ The letter
2 stated that “[f]or nearly two months, Mr. Musk has sought the data and information
3 necessary to ‘make an independent assessment of the prevalence of fake or spam
4 accounts on Twitter’s platform[,]” yet “Twitter has failed or refused to provide this
5 information.”
6

7
8 291. In response, the price of Twitter’s common stock fell 11.3%, or \$4.16, from
9 a closing price of \$36.81 on July 8, 2022, to close at \$32.65 on the next trading day, July
10 11, 2022.
11

12 292. On August 23, 2022, an article in the *Washington Post* publicly reported,
13 for the first time, Zatko’s whistleblower disclosure to the Federal government. The *Post*
14 published a partially redacted version of Zatko’s whistleblower complaint as well as two
15 internal Twitter documents attached as exhibits thereto, which revealed that Twitter had
16 misled investors and the public despite Zatko’s reports to the Board and the C-suite.
17
18

19 293. In response to this news, the price of Twitter’s common stock fell 7.32%, or
20 \$3.15, from a closing price of \$43.01 on August 22, 2022, to close at \$39.86 on August
21 23, 2022.
22

23 294. Twitter investors did not have to wait long to see governments’ response.
24 The next day, on August 24, 2022, the Senate Judiciary Committee announced “a full
25

26
27 ²³ See [https://www.sec.gov/Archives/edgar/data/1418091/](https://www.sec.gov/Archives/edgar/data/1418091/000110465922078413/tm2220599d1_ex99-p.htm)
28 [000110465922078413/tm2220599d1_ex99-p.htm](https://www.sec.gov/Archives/edgar/data/1418091/000110465922078413/tm2220599d1_ex99-p.htm).

1 Committee hearing to investigate allegations of widespread security failures at Twitter
2 and foreign state actor interference on Tuesday, September 13 at 10am.” That same day,
3 the data privacy authorities for both Ireland and France confirmed they were
4 investigating Zatko’s allegations. In connection with Zatko’s testimony, the Senate
5 Judiciary Committee made public dozens of internal Twitter documents attached to
6 Zatko’s whistleblower report, which confirm the truth of Zatko’s claims. In December
7 2022, *Bloomberg* reported that the FTC had intensified an investigation of Twitter that
8 had begun in Q3 2022, very close in time to Zatko’s revelations.
9
10
11

12 **VII. PRESUMPTION OF RELIANCE**

13 295. To the extent that Lead Plaintiffs allege that Defendants made affirmative
14 misstatements, Lead Plaintiffs will rely upon the presumption of reliance established by
15 the fraud-on-the-market doctrine in that, among other things:
16

- 17 a. Defendants made public misrepresentations or failed to disclose
18 material facts during the Class Period;
- 19 b. the omissions and misrepresentations were material;
- 20 c. the Company’s securities traded in an efficient market;
- 21 d. the misrepresentations alleged would tend to induce a reasonable
22 investor to misjudge the value of the Company’s publicly traded
23 securities;
24
25
26
27
28

- 1 e. Plaintiffs and other members of the Class purchased Twitter's
2 common stock between the time Defendants misrepresented or
3 failed to disclose material facts and the time the true facts were
4 disclosed, without knowledge of the misrepresented or omitted
5 facts;
6
7 f. Twitter's common stock met the requirements for listing and was
8 listed and actively traded on the NYSE, a highly efficient and
9 automated market;
10
11 g. as a regulated issuer, Twitter filed periodic public reports with the
12 SEC and the NYSE;
13
14 h. Twitter regularly communicated with public investors via
15 established market communication mechanisms, including regular
16 dissemination of press releases on the national circuits of major
17 newswire services and other wide-ranging public disclosures, such
18 as communications with the financial press and other similar
19 reporting services; and
20
21 i. Twitter was followed by many securities analysts employed by
22 major brokerage firms, including JPMorgan Chase & Co.,
23 Guggenheim Securities, LLC, Wells Fargo & Company, Jefferies
24 LLC, Piper Sandler & Co., JMP Securities LLC, Cowen and
25
26
27
28

1 Company, LLC, Wedbush Securities, Morgan Stanley & Co.
2 LLC, Barclays Bank PLC, UBS AG, Oppenheimer & Co. Inc.,
3 BMO Financial Group, and Deutsche Bank AG, all of which
4 wrote reports that were distributed to the sales force and certain
5 customers of their respective brokerage firm(s) and that were
6 publicly available and entered the public marketplace.
7
8

9 296. As a result of the foregoing, the market for Twitter's publicly traded
10 securities promptly digested current information regarding Twitter from publicly
11 available sources and reflected such information in the price of Twitter's publicly traded
12 securities. Under these circumstances, all persons and entities who or which purchased
13 or otherwise acquired Twitter's publicly traded securities during the Class Period
14 suffered similar injuries through their purchase of Twitter's publicly traded securities at
15 artificially inflated prices and thus, the presumption of reliance applies.
16
17
18

19 297. The material misrepresentations and omissions alleged herein would induce
20 a reasonable investor to misjudge the value of Twitter's publicly traded securities.
21

22 298. Without knowledge of the misrepresented or omitted material facts alleged
23 herein, Plaintiffs and other members of the Class purchased shares of Twitter's publicly
24 traded securities between the time Defendants misrepresented or failed to disclose
25 material facts, or concealed material risks, and the time the true facts were disclosed, or
26 the time such risks materialized.
27
28

1 299. To the extent that Defendants concealed or improperly failed to disclose
2 material facts regarding Twitter, Plaintiffs and other members of the Class are entitled to
3 a presumption of reliance in accordance with *Affiliated Ute Citizens of Utah v. United*
4 *States*, 406 U.S. 128, 153 (1972).
5

6 **VIII. INAPPLICABILITY OF STATUTORY SAFE HARBOR OR BESPEAKS**
7 **CAUTION DOCTRINE**

8 300. The protections applicable to forward-looking statements under certain
9 circumstances, including the statutory safe harbor provided by the PSLRA, do not apply
10 to any of the false or misleading statements alleged herein. The statements complained
11 of herein concerned then-present or historical facts or conditions that existed at the time
12 the statements were made.
13
14

15 301. To the extent any of the false or misleading statements alleged herein can be
16 construed as forward-looking, (a) they were not accompanied by meaningful cautionary
17 language identifying important facts that could cause actual results to differ materially
18 from those in the statements, and the generalized risk disclosures Defendants made were
19 not sufficient to shield Defendants from liability, and (b) the person who made each such
20 statement knew that the statement was untrue or misleading when made, or each such
21 statement was approved by an executive officer of Twitter who knew that the statement
22 was untrue or misleading when made.
23
24
25
26
27
28

1 **IX. CLASS ACTION ALLEGATIONS**

2 302. Plaintiffs bring this action as a class action pursuant to Federal Rule of Civil
3 Procedure 23(a) and (b)(3) on behalf of themselves and all persons or entities all persons
4 and entities who purchased or acquired publicly traded securities of Twitter from August
5 3, 2020 through August 23, 2022, both dates inclusive (the “Class Period”), and who
6 were damaged thereby. Excluded from the Class are: (i) Defendants; (ii) members of the
7 immediate family of any Individual Defendant; (iii) any person who was an officer or
8 director of Twitter during the Class Period; (iv) any entity in which any Defendant has or
9 had a controlling interest; (v) affiliates of Twitter; and (vi) the legal representatives,
10 affiliates, heirs, successors-in-interest, or assigns of any such excluded person in (i)-(v)
11 of this paragraph, in their capacities as such.
12
13
14
15

16 303. The members of the Class are so numerous that joinder of all members is
17 impracticable. During the Class Period, the Company’s common stock has actively
18 traded on the NYSE, and its other publicly traded securities traded actively. While the
19 exact number of Class members is unknown to Plaintiffs at this time and can be
20 ascertained only through appropriate discovery, Plaintiffs believe that there are
21 hundreds, if not thousands, of members in the Class and that such members are
22 geographically dispersed. Record owners and other members of the Class may be
23 identified from records maintained by Twitter or its transfer agent and may be notified of
24
25
26
27
28

1 the pendency of this action by mail, using the form of notice similar to that customarily
2 used in securities class actions.

3
4 304. Plaintiffs' claims are typical of the claims of members of the Class. All
5 members of the Class were similarly affected by Defendants' wrongful conduct as
6 complained of herein.

7
8 305. Plaintiffs will fairly and adequately protect the interests of the members of
9 the Class and has retained counsel competent and experienced in class and securities
10 litigation.

11
12 306. Common questions of law and fact exist as to all members of the Class and
13 predominate over any questions solely affecting individual members of the Class.
14 Among the questions of law and fact common to the Class are:

- 15
16 a. Whether the federal securities laws were violated by Defendants
17 as alleged herein;
18
19 b. Whether the statements made to the investing public during the
20 Class Period contained material misrepresentations;
21
22 c. Whether Defendants omitted material facts that they had a duty to
23 disclose;
24
25 d. Whether Defendants knew or recklessly disregarded that their
26 statements were false and misleading;

e. Whether Defendants acted with the intent to defraud Class members regarding the true value of Twitter's publicly traded securities;

f. Whether the Individual Defendants were controlling persons of Twitter; and

g. Whether and to what extent members of the proposed Class suffered losses due to the acts and omissions alleged herein.

307. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because, among other things, joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation may make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

X. Counts

COUNT I

(Violations of Section 10(b) of the Exchange Act, and Rule 10b-5 Thereunder, Against Defendants)

308. This Count is asserted pursuant to Section 10(b) of the Exchange Act, and Rule 10b-5 promulgated thereunder by the SEC, against all Defendants.

309. As alleged herein, throughout the Class Period, Defendants, individually and in concert, directly and indirectly, by the use of the means or instrumentalities of

1 interstate commerce, the mails and/or the facilities of national securities exchanges,
2 made untrue statements of material fact and/or omitted to state material facts necessary
3 to make their statements not misleading and carried out a plan, scheme and course of
4 conduct, in violation of Section 10(b) of the Exchange Act and Rule 10b-5 promulgated
5 thereunder. Defendants intended to and did, as alleged herein, (i) deceive the investing
6 public, including Plaintiffs and members of the Class; (ii) artificially inflate and maintain
7 the price of Twitter's publicly traded securities; and (iii) cause Plaintiffs and members of
8 the Class to purchase Twitter's publicly traded securities at artificially inflated prices.
9
10
11

12 310. The Individual Defendants were individually and collectively responsible
13 for making the false and misleading statements and omissions alleged herein and having
14 engaged in a plan, scheme, and course of conduct designed to deceive Plaintiffs and
15 members of the Class, by virtue of having made public statements and prepared,
16 approved, signed, and/or disseminated documents that contained untrue statements of
17 material fact and/or omitted facts necessary to make the statements therein not
18 misleading.
19
20
21

22 311. As set forth above, Defendants made their false and misleading statements
23 and omissions and engaged in the fraudulent activity described herein knowingly and
24 intentionally, or in such a deliberately reckless manner as to constitute willful deceit and
25 fraud upon Plaintiffs and the other members of the Class who purchased Twitter's
26 publicly traded securities during the Class Period.
27
28

1 meaning of Section 20(a) of the Exchange Act as alleged herein. By virtue of their
2 leadership positions, the Individual Defendants had the power to influence and control
3 and did, directly or indirectly, influence and control the decision making of the
4 Company, including the content and dissemination of the various statements which Lead
5 Plaintiffs contend were false and misleading. The Individual Defendants were provided
6 with or had unlimited access to the Company's internal reports, press releases, public
7 filings, and other statements alleged by Plaintiffs to be misleading prior to or shortly
8 after these statements were issued, and had the ability to prevent the issuance of the
9 statements or cause them to be corrected.

13 316. In particular, the Individual Defendants had direct involvement in and
14 responsibility over the day-to-day operations of the Company and, therefore, are
15 presumed to have had the power to control or influence the particular transactions giving
16 rise to the securities violations as alleged herein.

19 317. By reason of such wrongful conduct, the Individual Defendants are liable
20 pursuant to Section 20(a) of the Exchange Act. As a direct and proximate result of the
21 Individual Defendants' wrongful conduct, Plaintiffs and the other members of the Class
22 suffered damages in connection with their purchases of the Company's shares during the
23 Class Period.

26 **XI. PRAYER FOR RELIEF**

27 WHEREFORE, Plaintiffs demand judgment against Defendants as follows:

A. Determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, certifying Plaintiffs as class representative, and appointing Plaintiffs' counsel as Counsel for the Class;

B. Awarding compensatory damages in favor of Plaintiffs and the other Class members against all Defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be determined at trial, including prejudgment and post-judgment interest, as allowed by law;

C. Awarding Plaintiffs and the Class their reasonable attorneys' fees, expert fees, and other costs incurred in this action; and

D. Awarding such equitable, injunctive, and other relief as the Court may deem just and proper.

XII. JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: February 13, 2022

Respectfully submitted,

POMERANTZ LLP

By: s/ Jonathan D. Park

THE ROSEN LAW FIRM, P.A.

POMERANTZ LLP

Laurence M. Rosen (SBN 219683)
355 South Grand Avenue, Suite 2450
Los Angeles, CA 90071
Telephone: (213) 785-2610
Facsimile: (213) 226-4684
Email: lrosen@rosenlegal.com

Jeremy A. Lieberman (*pro hac vice*
forthcoming)
Jonathan D. Park (*pro hac vice*)
600 Third Avenue, 20th Floor
New York, New York 10016
Telephone: (212) 661-1100

Jonathan Horne (*pro hac vice* forthcoming)
275 Madison Avenue, 40th Floor
New York, New York 10016
Telephone: (212) 686-1060
Facsimile: (212) 202-3827
jhorne@rosenlegal.com

Facsimile: (212) 661-8665
jalieberman@pomlaw.com
jpark@pomlaw.com

Jennifer Pafiti (SBN 282790)
1100 Glendon Avenue, 15th Floor
Los Angeles, California 90024
Telephone: (310) 405-7190
Facsimile: (212) 661-8665
jpafiti@pomlaw.com

*Counsel for Court-Appointed Lead
Plaintiff William Baker, Additional
Plaintiffs Lenard Roque and Amolkumar
Vaidya, and Co-Lead Counsel for the Class*

*Counsel for Court-Appointed Lead
Plaintiff William Baker, Additional
Plaintiffs Mohammed Thaseen and Jill
Sligay, and Co-Lead Counsel for the Class*

**BRONSTEIN, GEWIRTZ &
GROSSMAN, LLC**

Peretz Bronstein
60 East 42nd Street, Suite 4600
New York, NY 10165
Telephone: (212) 697-6484
Facsimile: (212) 697-7296
peretz@bgandg.com

*Counsel for Additional Plaintiff
Mohammed Thaseen*

Appendix A

**CERTIFICATION PURSUANT
TO FEDERAL SECURITIES LAWS**

1. I, Jill Sligay, make this declaration pursuant to Section 21D(a)(2) of the Securities Exchange Act of 1934 (“Exchange Act”) as amended by the Private Securities Litigation Reform Act of 1995.

2. I have reviewed the initial complaint and draft amended complaint against Twitter, Inc. (“Twitter”) and other defendants, and I authorize the filing of the amended complaint.

3. I did not purchase or acquire Twitter securities at the direction of plaintiffs’ counsel or in order to participate in any private action arising under the Securities Act or Exchange Act.

4. I am willing to serve as a representative party on behalf of a Class of investors who purchased or otherwise acquired Twitter securities during the class period, including providing testimony at deposition and trial, if necessary. I understand that the Court has the authority to select the most adequate lead plaintiff in this action.

5. The attached sheet lists all of my transactions in Twitter securities during the Class Period as specified in the amended complaint.

6. During the three-year period preceding the date on which this Certification is signed, I have not served or sought to serve as a representative party on behalf of a class under the federal securities laws.

7. I agree not to accept any payment for serving as a representative party on behalf of the class as set forth in the amended complaint, beyond my pro rata share of any recovery, except such reasonable costs and expenses directly relating to the representation of the class as ordered or approved by the Court.

8. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed: February 10, 2022

DocuSigned by:



(Signature)

E7AE0EBCFEB8496...

Jill Sligay

(Type or Print Name)

Twitter Inc. (TWTR)

Jill Sligay

List of Purchases and Sales

Transaction Type	Date	Number of Shares/Unit	Price Per Share/Unit
Purchase	4/25/2022	9.80392	\$51.0000
Purchase	4/25/2022	9.80392	\$51.0000
Purchase	4/26/2022	19.39487	\$51.5600

Certification and Authorization of Named Plaintiff Pursuant to Federal Securities Laws

The individual or institution listed below (the "Plaintiff") authorizes and, upon execution of the accompanying retainer agreement by The Rosen Law Firm P.A., retains The Rosen Law Firm P.A. to file an action under the federal securities laws to recover damages and to seek other relief against Twitter, Inc. (Whistleblower) The Rosen Law Firm P.A. will prosecute the action on a contingent fee basis not to exceed one-third of the recovery and will advance all costs and expenses. All payments of fees and expenses shall be made only after Court review and approval. The Twitter, Inc. (Whistleblower) Retention Agreement provided to the Plaintiff is incorporated by reference herein and is effective, upon execution and delivery by The Rosen Law Firm P.A.

First Name: Lenard
Middle Initial: C
Last Name: Roque
Mailing Address: Redacted
City:
State:
Zip Code:
Country:
Phone:
Email Address:

Plaintiff certifies that:

1. Plaintiff has reviewed a complaint and authorized its filing or the filing of an amended complaint.
2. Plaintiff did not acquire the security that is the subject of this action at the direction of plaintiff's counsel or in order to participate in this private action or any other litigation under the federal securities laws.
3. Plaintiff is willing to serve as a representative party on behalf of a class, including providing testimony at deposition and trial, if necessary.
4. Plaintiff represents and warrants that he/she/it is fully authorized to enter into and execute this certification.
5. Plaintiff will not accept any payment for serving as a representative party on behalf of the class beyond Plaintiff's pro rata share of any recovery, except such reasonable costs and expenses (including lost wages) directly relating to the representation of the class as ordered or approved by the court.
6. Plaintiff has made no transaction(s) during the Class Period in the debt or equity securities that are the subject of this action except those set forth below:

Purchases:

Type of Security	Buy Date	# of Shares	Price per Share
Common Stock	4/18/22	692	\$46.64
Type of Security	Buy Date	# of Shares	Price per Share
Common Stock	4/18/22	42	\$46.69
Type of Security	Buy Date	# of Shares	Price per Share
Common Stock	4/5/22	55	\$51.51
Type of Security	Buy Date	# of Shares	Price per Share
Common Stock	4/18/22	127	\$46.64

Sales:

Type of Security	Sale Date	# of Shares	Price per Share
Common Stock	9/1/22	692	\$38.72

Type of Security	Sale Date	# of Shares	Price per Share
Common Stock	9/1/22	42	\$38.67

Type of Security	Sale Date	# of Shares	Price per Share
Common Stock	9/1/22	55	\$38.62

Type of Security	Sale Date	# of Shares	Price per Share
Common Stock	9/1/22	127	\$38.68

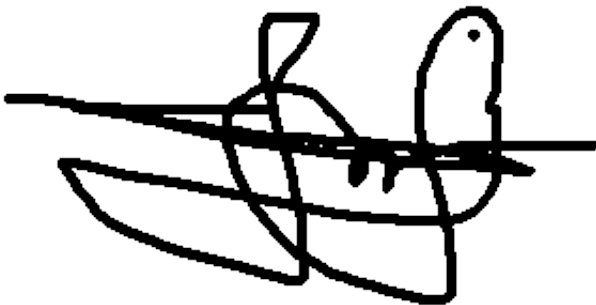
I have not sought to serve as a representative party on behalf of a class under the federal securities laws during the last three years, except if set forth below.

Not applicable

I declare and certify under penalty of perjury, under the laws of the United States of America, that the foregoing information is true and correct. **YES**

By Signing below and submitting this certification form electronically, I intend to sign and execute this certification pursuant to California Civil Code Section 1633.1, et seq. - and the Uniform Electronic Transactions Act and retain the Rosen Law Firm, P.A. to proceed on Plaintiff's behalf, on a contingent fee basis. **YES**

Date of signing: 11/02/2022 01:43:48 at Eastern Standard Time, USA

A handwritten signature in black ink, consisting of a stylized, cursive script. The signature is written over a horizontal line.