PUBLIC

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Andrew N. Ferguson, Chair**
Mark Meador

In the Matter of **Twitter, Inc.** **a corporation;**	**Docket No. C-4316**

PETITION TO REOPEN AND SET ASIDE OR, IN THE ALTERNATIVE, MODIFY DECISION AND ORDER

Pursuant to Section 5(b) of the Federal Trade Commission Act, 15 U.S.C. § 45(b), and Section 2.51 of the Federal Trade Commission Rules of Practice, 16 C.F.R. § 2.51, Respondent X Corp. ("X" or the "Company") respectfully petitions the Commission to reopen this proceeding and promptly set aside or, at a minimum, modify the Commission's Decision and Order entered on May 26, 2022 (the "Order").

Since 2011, the Federal Trade Commission has placed the Company under a twenty-year consent order, overseeing how it stores and secures user information.[1] In 2022, the Commission doubled down, extending the 2011 Order for another twenty years and mandating a highly-reticulated compliance architecture, new restrictions on data use, regular third-party exhaustive assessments, and standing subpoena-like powers.[2] To date, the 2022 Order has forced the

[1] Decision and Order, *In re Twitter, Inc.*, Docket No. C-4316, 151 F.T.C. 162 (Mar. 2, 2011) [hereinafter "2011 Order"].

[2] Ex. A, Modified Decision and Order, *In re Twitter, Inc.*, Docket No. C-4316 (F.T.C. May 26, 2022) [hereinafter "2022 Order"]. *See also* Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. May 26, 2022), Dkt. 11.

Company to divert close to $17 million to paperwork. The predicate for this extraordinary extension was a single category of alleged misconduct: that Twitter had used email addresses and phone numbers collected for account-security purposes to improve the targeting of advertisements, without adequately disclosing that use. The conduct was not the product of a deliberate scheme to deceive. It was the result of back-end engineering decisions that failed to adequately segregate data—a failure that Twitter itself identified, voluntarily disclosed to the public, and promptly corrected, all before the Order was ever negotiated. No user data was shared with advertisers. No consumer was found to have suffered any cognizable injury. And multiple California courts evaluating the identical conduct later held, on the merits and with prejudice, that Twitter's Privacy Policy actually did disclose the challenged use in clear, unambiguous terms.

This is not a close case. After more than fifteen years of Commission oversight, the Order should be set aside without delay. The reasons are compelling and mutually reinforcing.

First, the Order was imposed on a company that no longer exists. Every individual responsible for the underlying failures has left, and X has since built a world-class privacy and data-protection program that its own personnel regard as a crucial element of the Company's culture. There is no consumer-protection rationale to maintain a twenty-year regulatory regime over an entity that did not commit the underlying violations, and has never violated the Order.

Second, the Order no longer serves any valid regulatory purpose, and so imposes millions of dollars in needless costs. Its obligations are duplicative of protections already required by domestic and international privacy regimes as well as industry-recognized frameworks to which X independently adheres. The factual foundation of the FTC's complaint has been dismantled. And the Order's staggering costs—imposed on both the Company and on the Commission itself—are unjustifiable.

Third, setting aside the Order safeguards First Amendment values. X is the nation's most prominent platform for open public discourse. Maintaining a sweeping consent decree over such a platform creates a permanent mechanism through which future regulators can pressure the Company over the viewpoints it hosts. Indeed, during the last administration, the FTC weaponized the Order's demand-letter authority to interrogate X about core First Amendment activity with no meaningful connection to privacy compliance.

Fourth, terminating the Order is critical to advancing American leadership in artificial intelligence. X operates at the center of a family of companies—including xAI—that are at the forefront of America's AI ambitions. The Order diverts engineering resources from innovation to compliance paperwork and is precisely the kind of outdated encumbrance that President Trump's Executive Order 14179 and subsequent AI Action Plan were designed to address.[3]

The Commission should set it aside immediately, or, in the alternative, modify it to terminate before the end of this calendar year.

BACKGROUND

I. The 2011 Order.

The Commission's regulatory oversight of X's predecessor Twitter, Inc. began with a consent order entered on March 2, 2011, fifteen years and several technological revolutions ago.[4] The FTC investigated discrete incidents in which hackers gained access to Twitter's internal systems and charged that Twitter had violated Section 5 of the FTC Act by failing to use reasonable security measures to protect nonpublic user data from unauthorized access, by failing to honor

[3] Exec. Order No. 14,179, 90 Fed. Reg. 8,741 (Jan. 23, 2025); The White House, *Winning the Race: America's AI Action Plan* 3–4 (July 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

[4] 2011 Order.

users' privacy choices, and by misrepresenting the security measures it had in place.[5] These were specific, bounded failures—the growing pains of a young technology company that had not yet built the kind of institutional security infrastructure its rapid growth demanded.

The 2011 Order required Twitter to establish a "comprehensive information security program" meeting certain specified parameters.[6] It mandated that Twitter obtain biennial assessments of that program from qualified, independent third-party professionals.[7] And it prohibited Twitter from misrepresenting the extent to which it maintained and protected the security and privacy of nonpublic consumer information.[8]

II. The Proceedings Leading to the 2022 Order

In October 2019, Twitter publicly and voluntarily disclosed that, due to certain back-end engineering decisions, some email addresses and phone numbers that users had provided for account security purposes—such as two-factor authentication, password recovery, and re-authentication—may have been used unintentionally for advertising purposes.[9] Specifically, Twitter's advertising systems ingested these contact details and used them to match users against advertiser-uploaded audience lists, thereby improving the targeting of ads served to those users.[10] It affected a potentially large number of users, though critically, the data at issue was never actually shared with advertisers. The company used the information internally to improve the targeting of its *own* advertising products.[11]

---

[5] Compl. ¶¶ 11–12, *In re Twitter, Inc.*, Docket No. C-4316 (F.T.C. Mar. 2, 2011).
[6] 2011 Order ¶ II.
[7] *Id*. ¶ III.
[8] *Id*. ¶ I.
[9] Twitter Support (@TwitterSupport), Twitter (Oct. 8, 2019, 4:02 PM), https://twitter.com/twittersupport/status/1181661080033955840; *see also* Concurring Statement of Comm'r Christine S. Wilson & Comm'r Noah Joshua Phillips at 6, *In re Twitter, Inc.*, Matter No. 2023062 (May 25, 2022) (noting Twitter's public disclosure "in October 2019") ["Wilson & Phillips Statement"].
[10] Compl. ¶¶ 26–27, *United States v. Twitter, Inc.*, No. 3:22-cv-03070 (N.D. Cal. May 25, 2022), Dkt. 1.
[11] *Id.* ¶ 26 (noting that Twitter used the information to match users against advertiser-uploaded audience lists

Twitter's disclosure was voluntary and transparent. The Company promptly began to remediate the issue internally.[12] Twitter's privacy policy, moreover, had already notified users that contact information would be used for advertising purposes, a point that would prove significant in subsequent litigation.[13]

Nonetheless, the FTC investigated. Over the next two years, the Commission sent approximately fifteen demand letters to Twitter.[14] On May 25, 2022, the Department of Justice and the FTC filed a complaint in the Northern District of California alleging that Twitter had violated the 2011 Order and Section 5 of the FTC Act by misrepresenting the extent to which it maintained and protected the privacy of nonpublic consumer information.[15] The following day, the Court entered a Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, imposing a $150 million civil penalty and the comprehensive set of injunctive provisions discussed below.[16] The Stipulated Order was entered into with Twitter's prior management, before the closing of Elon Musk's acquisition of the company in October 2022.

Significantly, the same underlying conduct also gave rise to private class action litigation. But the courts there *rejected* the claims against Twitter in full. In *Yeh v. Twitter, Inc.*, No. CGC-23-605100 (Cal. Super. Ct. May 31, 2024), the trial court dismissed the putative class action with prejudice on the pleadings.[17] The California Court of Appeal affirmed, holding that Twitter's

through its Tailored Audiences and Partner Audiences services, but did not share the underlying contact data with advertisers).

[12] *See* Wilson & Phillips Statement at 6.

[13] *See Yeh v. Twitter, Inc.*, No. A170843, 2026 WL 44933, at *3–4 (Cal. Ct. App. Jan. 7, 2026), *rev. granted* (Mar. 25, 2026).

[14] *See, e.g.*, Exs. 1–13 to X Corp.'s Mot. for Protective Order & Relief from Consent Order, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. Jul. 13, 2023), Dkt. 17 (attaching representative demand letters).

[15] Compl., *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. May 25, 2022), Dkt. 1.

[16] Stipulated Order for Civil Penalty, Monetary J., and Injunctive Relief, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. May 26, 2022), Dkt. 11.

[17] *Yeh*, 2026 WL 44933, at *5.

Privacy Policy "expressly provides, in several distinct provisions, that Twitter uses its users' personal information, including their email address and phone number, for security *and* advertising/marketing purposes" in clear and unambiguous terms.[18] The court found that Twitter's use of the data for targeted advertising was, as a matter of law, neither an unlawful nor an unfair business practice, and that users had permitted Twitter to do so when they agreed to the company's Privacy Policy.[19]

III. The 2022 Order's Twenty-Year Extension of Commission Oversight

At base, the 2022 Order requires a comprehensive information security program and a comprehensive privacy program (already required under State and Global privacy laws) to be continually assessed through onerous third-party audits over a term of twenty years. This is a structure that the Commission itself acknowledged was modeled on the obligations imposed on Facebook following allegations that the company had engaged in a far more egregious course of conduct.[20]

The third-party assessments, which must be approved by the Commission, determine whether the Company has implemented and maintained the required program, assess the effectiveness of each element, identify any gaps or weaknesses, and address the status of any

---

[18] *Id.* at *3–4.

[19] *Id.* at *5–8. The California Supreme Court granted review limited to the narrow question of standing under California's Unfair Competition Law. (No. S295210.) The Court of Appeal's thorough analysis regarding the adequacy of the Privacy Policy disclosures remains highly persuasive and directly refutes the FTC complaint's core allegation that users were not adequately informed of the challenged use of their contact information.

[20] Wilson & Phillips Statement at 2 (noting that the requirement for both a privacy and an information security program was "a dual obligation we first imposed in our 2019 enforcement action against Facebook"). Although the Commission had Meta's consent decree in mind, terminating the Order applied to X would not require the Commission to rethink Meta's. The conduct in this case stands in sharp contrast to the conduct alleged in Meta's. Twitter's conduct was voluntarily disclosed and was internally remediated, the company was subsequently acquired by new management, and the individuals responsible for the underlying issue departed. By contrast, the FTC alleged that Meta had "repeatedly violated its privacy promises," continued to breach its requirements, and "pose[d] substantial risks to the public." *See* Order to Show Cause at 4–5, 9–11, *In re Facebook, Inc.*, Docket No. C-4365 (F.T.C. May 3, 2023).

previously identified deficiencies.[21] The Company must cooperate fully with the assessor and must not misrepresent any material fact.[22] The Order also prescribes *how* the Company must make decisions regarding the collection, maintenance, use, disclosure, or provision of user information, limiting such decision-making to a small group of designated officers.[23]

Beyond these duplicative programmatic requirements, the Order imposes extensive recordkeeping obligations spanning twenty years,[24] and broad compliance-monitoring provisions that authorize the Commission to demand additional compliance reports, conduct depositions, and obtain discovery using the full range of the Federal Rules of Civil Procedure—all without further leave of court.[25]

Perhaps most consequentially, the Order authorizes Commission staff to issue interrogatories and document demands that the Company must answer, under penalty of perjury, within fourteen days.[26] This demand-letter authority operates as a standing subpoena power, exercisable at any time, on any subject arguably connected to the Order, with no judicial oversight and no meaningful procedural protections. As subsequent events would demonstrate, the breadth of this authority invites precisely the kind of overreach that the Commission's own members have cautioned against.

IV. The Company Today

The entity subject to this Order is not the company that entered into it. On April 25, 2022, Elon Musk signed an agreement to acquire Twitter, Inc. and take it private.[27] The transaction

[21] 2022 Order § VI.D.1–4.
[22] *Id*. § VII.
[23] *Id*. § V.E.4(c).
[24] *Id*. § XII.
[25] *Id*. § XIII.A.
[26] *Id*.
[27] Cara Lombardo et al., *Twitter Accepts Elon Musk's Offer to Buy Company in $44 Billion Deal*, Wall St. J. (Apr. 25, 2022), https://www.wsj.com/articles/twitter-and-elon-musk-strike-deal-for-takeover-11650912837.

closed on October 27, 2022.[28] What followed was more than a mere change in corporate control. It was a fundamental transformation of the company's leadership, mission, organizational structure, technology infrastructure, and relationship to its users.

As Twitter itself explained to the FTC in December 2022, the company was "undergoing a fundamental transformation" involving "a substantial overhaul of its organizational structure, budgeting, revenue-generation priorities, and other fundamental aspects of the business."[29] Twitter, Inc. was merged into X Corp.[30] The company was rebranded. Its corporate structure was reconstituted. The board of directors that approved the 2022 Order was dissolved when the company went private.[31] The senior executives who had overseen the compliance with the 2011 Order—including the Chief Privacy Officer, the Chief Security Officer, the head of Human Resources, and the General Counsel's office—departed in the weeks and months following the acquisition.[32]

Under new ownership, the Company fundamentally reoriented its approach to free expression. One of Mr. Musk's first priorities was to recommit the platform to open discourse—a commitment that required a reckoning with Twitter's historical content-moderation decisions and its entanglement with government censors. That reckoning occurred principally through the Twitter Files, in which Mr. Musk invited independent journalists to examine internal Twitter

---

[28] *See* Letter from Daniel R. Koffmann, Quinn Emanuel, to Reenah L. Kim, FTC at 1 (Dec. 14, 2022), Ex. 5 to X Corp.'s Mot. for Protective Order, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. Jul. 13, 2023), Dkt. 18-5 (confirming "Elon Musk acquired control of the Company on October 27, 2022") [hereinafter "Koffmann Letter"].

[29] *Id.*

[30] *See* Delaware Secretary of State, Certificate of Merger of X Corp. (Mar. 15, 2023), *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. Jul. 13, 2023), Dkt. 18-6.

[31] *See* Koffmann Letter at 9 (confirming that "Mr. Musk has served as the sole director" since October 27, 2022).

[32] *See id.* at 5, 7–9 (documenting that the Chief Privacy Officer resigned November 10, 2022; the Chief Information Security Officer resigned November 9, 2022; the General Counsel position was unoccupied since October 27, 2022; and the Chief Compliance Officer resigned November 9, 2022); Dep. of David Roque at 38:15–40:7, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. Jun. 21, 2023), Dkt. 18-14.

communications.[33] The results were alarming. The Twitter Files exposed routine government interference at the behest of Biden Administration political operatives, with complicity from former Twitter executives, that resulted in tendentious content moderation—including the suppression of views from doctors and scientific experts that conflicted with official White House positions.[34]

X has ended Twitter's practice of political censorship and implemented innovations such as Community Notes—a crowdsourced approach to fact-checking that has become an industry standard and provides a fast, neutral, and reliable means of adding context to posts.[35] The Company has expended substantial resources to resist censorship demands from governments around the world, repeatedly refusing pressure from foreign regulators who seek to suppress disfavored viewpoints and defending users' rights to speak freely despite significant legal and financial risks.[36] X opposed Special Counsel Jack Smith's improper efforts to access President Trump's user data all the way to the United States Supreme Court,[37] and obtained a unanimous decision from the D.C. Circuit reversing a nondisclosure order that had prevented the Company from

[33] *See* Matt Taibbi (@mtaibbi), Twitter (Dec. 2, 2022) (publishing the first installment of the "Twitter Files"); Bari Weiss (@bariweiss), Twitter (Dec. 8, 2022) (publishing further installments regarding internal content-moderation deliberations).

[34] *See* Michael Shellenberger (@shellenberger), Twitter (Dec. 26, 2022) (reporting on FBI and government-agency coordination with Twitter to suppress content); David Zweig (@davidzweig), Twitter (Dec. 26, 2022) (documenting the suppression of expert medical opinions that diverged from official White House COVID-19 positions).

[35] X Corp., *Community Notes Guide*, X, https://communitynotes.x.com/guide/en/about/introduction (last visited Apr. 23, 2026). To prevent bias, Community Notes appear on posts only if users who have had generally divergent opinions agree on the content of a particular Note.

[36] *See, e.g.*, X Corp., *Global Government Information Requests Report*, X (2024), https://transparency.x.com (documenting X's record of challenging government demands and disclosing the frequency with which such demands are received and contested).

[37] *See In re Sealed Case*, 77 F.4th 815, 821 (D.C. Cir. 2023), *pet. for rehearing en banc denied sub nom. In re Search of Info. Stored at Premises Controlled by Twitter, Inc.*, No. 23-5044, 2024 WL 158766 (D.C. Cir. Jan. 16, 2024), *cert. denied sub nom. X Corp. v. United States*, 145 S. Ct. 159 (2024).

disclosing to two former FBI agents that they were being persecuted by the Biden FBI for blowing the whistle to Congress.[38]

The Company's approach to user privacy and data protection has likewise been rebuilt from the ground up. X established comprehensive privacy and information security programs built on [redacted], combined with Generally Accepted Privacy Principles.[39] These programs are governed by six foundational principles: a proactive approach to privacy; privacy as the default; privacy embedded into design; no compromise on functionality; end-to-end lifecycle security; and visibility and transparency.[40]

V. X's Compliance with the Order

X has complied with the 2022 Order fully. The record of compliance is documented, independently verified, and unambiguous.

As noted, the 2022 Order required the Company to implement and maintain a comprehensive privacy and information security program meeting the specifications of Section V.

[redacted]

[38] *In re Sealed Case*, 144 F.4th 329 (D.C. Cir. 2025) (unanimously reversing nondisclosure order that had prevented the company from informing the targets of the investigation).

[39] *See* Ex. B, [redacted]

[40] *Id.* [redacted]

[41] *Id.* [redacted]

[redacted]

The Order requires biennial independent assessments of the Company's compliance with Section V, to be conducted by a qualified third-party professional. X has now completed two full assessment cycles—both conducted by FTI Consulting, Inc., which the Commission approved as the Company's independent assessor following EY's resignation in early 2023.[43] For the most recent two-year period—from May 26, 2023, through May 25, 2025—FTI conducted a comprehensive assessment encompassing document reviews, personnel interviews, sampling, and testing across the full inventory of controls.[44]

The results were clear. FTI found that X "implemented and maintained the Program required by Provision V of the Order."[45] The Program, as designed, "provides sufficient coverage across all relevant privacy and information security domains and is in alignment with the [redacted], respectively, upon which the Program is based."[46] The assessment found no instances of material noncompliance with the 2022 Order.

The assessment confirmed the strength of X's approach across every major compliance domain. X's own risk assessments were found to "meet the requirements of the Order."[47] X's defense-in-depth information security strategy was found to be "reasonably designed to protect against threats and attack vectors with multiple layers of Controls."[48] And FTI noted that "X

[42] *Id.*
[43] *Id.* [redacted]
[44] *Id.* [redacted]
[45] *Id.* [redacted]
[46] *Id.* [redacted]
[47] *Id.* [redacted]
[48] *Id.* [redacted]

leadership has emphasized its promotion of a security and privacy-minded culture throughout the organization."[49]

Beyond the independent assessments, X has satisfied every other compliance obligation the Order imposes. The $150 million civil penalty has been paid in full, X has submitted all required certifications and compliance reports, and it has reported covered incidents within the required timeframes. It has responded to more than two hundred of the Commission's demand letters since the acquisition—producing more than 22,000 documents. It has made personnel available for depositions. And it has done all of this while simultaneously rebuilding the Company from the ground up.

The totality of the evidence, as FTI concluded, "demonstrated X's commitment to maintaining industry-standard privacy and information security programs."[50]

ARGUMENT

Section 5(b) of the FTC Act provides that the Commission may reopen and modify an order when the Commission determines that "conditions of fact or of law have so changed as to require such action *or* if the public interest shall so require." 15 U.S.C. § 45(b) (emphasis added); *see also* 16 C.F.R. § 2.51(b). Either basis suffices, and here each independently warrants the Commission reopening and setting aside or, in the alternative, modifying the order.

I. Changed Conditions of Law and Fact Warrant Reopening and Setting Aside or, in the Alternative, Modifying the Order.

There are at least three ways in which "conditions of fact or of law have so changed" as to warrant the 2022 Order's prompt reopening and modification. 15 U.S.C. § 45(b).

[49] *Id.*
[50] *Id.* [redacted]

A. The Order has Served its Remedial Purpose.

The Commission has long recognized that when an order has achieved its remedial purpose, continuing it in effect is no longer warranted. *See, e.g.*, *In re Conoco Inc.*, 152 F.T.C. 1042 (2011) (granting modification when "it is clear that the Order has achieved its remedial objectives"); *In re Magnavox Co.*, 102 F.T.C. 807 (1983) (setting aside restrictions that "appear to have served their remedial purposes").

The record since 2022 establishes conclusively that the Order has served its remedial purpose and thus should not be allowed to remain in effect a moment longer.

The 2022 Order was designed to remedy a specific, identified harm: that Twitter, under prior ownership and management, had used email addresses and phone numbers collected for account-security purposes—two-factor authentication, password recovery, and re-authentication—to serve targeted advertisements, without adequately disclosing that use to affected users. The conduct at issue lasted from approximately May 2013 to September 2019 and was voluntarily disclosed and internally remediated by the company before the Order was even negotiated.[51] The Order then imposed an additional comprehensive set of requirements to ensure that the company could not use consumer data in ways inconsistent with its representations.

That objective has been achieved. FTI's assessment confirmed that X maintains technical and administrative procedures designed to prevent the collection, maintenance, use, disclosure, or access to consumer data—going beyond the limitations identified in the Order's product-review requirements.[52] [redacted]

[redacted]

[51] Compl. ¶ 27, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. May 25, 2022), Dkt. 1; Wilson & Phillips Statement at 6.

[52] [redacted]

[redacted] The very practices that led to the Order—the commingling of security-purpose data with advertising systems—have been structurally eliminated.

Moreover, X's privacy and information security programs are comprehensive, independently grounded programs that would survive and continue to operate in the Order's absence. To wit, many of the ways X has complied with the Order are how X complies with the EU's General Data Protection Regulation (GDPR), India's Personal Data Protection Act, Brazil's *Lei Geral de Proteção de Dados*, and the California Consumer Privacy Act.[56] Beyond these comprehensive statutory regimes, X independently adheres to industry-recognized frameworks that track and often exceed the Order's requirements. X's Privacy and Data Protection Program is built on [redacted][57] X's Information Security Program is likewise based on the [redacted]

[53] *Id.* [redacted]
[54] *Id.* [redacted]
[55] *Id.* [redacted]
[56] For instance, the GDPR mandates Data Protection Impact Assessments before a new program or service is introduced, a requirement duplicative of the Order's Section V privacy reviews.
[57] [redacted]
[58] *Id.* [redacted]

Indeed, FTI's independent assessment noted that "the totality of the Controls outlined in the Program demonstrated X's commitment to maintaining industry-standard privacy and information security programs."[59] X's privacy and security personnel view these programs as "crucial tenets of the company culture in order to achieve long-term success and trust with Users."[60] These are programs built on internationally recognized standards that X maintains because they are foundational to its business, its relationships with its more than half a billion monthly users, and its legal compliance with the global regulatory landscape in which it operates.[61] Maintaining a separate, twenty-year FTC-specific overlay in this environment serves no unique consumer-protection purpose.

The Order has accomplished what it set out to do. Twitter paid its penalty in full, and X has not committed any violation—or near violation—of its terms. Nor do the critical safeguards of users' personal information any longer depend on the continued enforcement of the Order. The Order has served its purpose, and the Commission should set it aside without delay.

B. The Factual and Legal Predicate for the Order Has Been Rejected.

The factual and legal predicate for the Order has been rejected in subsequent litigation evaluating the very same underlying conduct. Under the FTC's 2022 complaint, the theory of harm was straightforward: Twitter had "misrepresented to users" the extent to which it maintained and protected the privacy of their contact information by collecting telephone numbers and email addresses for account-security purposes—two-factor authentication, account recovery, and re-authentication—while failing to disclose that it "also used user contact information to aid

[59] *Id.*
[60] *Id.* [redacted]
[61] As described in Part I.A *supra*, these programs will also persist beyond the term of the Order because they satisfy the demands of overlapping legal regimes around the world.

advertisers in reaching their preferred audiences."[62] The complaint alleged that this failure to disclose was a deceptive act or practice in violation of Section 5 of the FTC Act and the 2011 Order's prohibition on misrepresenting the extent to which the company maintained and protected the privacy of nonpublic consumer information.[63]

The Order's factual premise has been squarely rejected. In *Yeh v. Twitter, Inc.*, a California trial court dismissed with prejudice a putative class action arising from the identical underlying conduct.[64] The California Court of Appeal unanimously affirmed, holding that Twitter's Privacy Policy actually *did* disclose its use of user contact information for advertising purposes—and did so in clear, unambiguous terms.[65] There was thus no basis for the Commission's finding that Twitter had misrepresented its data policies. The court examined each relevant provision of the Privacy Policy and concluded that it "expressly provides, in several distinct provisions, that Twitter uses its users' personal information, including their email address and phone number, for security and advertising/marketing purposes."[66] Specifically, the court pointed to Section 1.3, which informed users that Twitter uses their contact information "to authenticate your account and keep it—and our services—secure" as well as "*to market to you* as your country's laws allow"; Section 2.6, which stated that Twitter uses "the information described in this Privacy Policy *to help make our advertising more relevant to you*"; and Section 2.10, which gave users the ability to control "[w]hether we show you interest-based ads on and off Twitter."[67] On that basis, the court rejected each of the plaintiff's claims.

---

[62] Compl. ¶ 2, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. May 25, 2022), Dkt. 1.
[63] *Id.* ¶¶ 60–96.
[64] No. CGC-23-605100 (Cal. Super. Ct. May 31, 2024).
[65] *Yeh*, 2026 WL 44933, at *3–5 (emphasis in original). The California Supreme Court's grant of review limited to the narrow question of standing under California's Unfair Competition Law does not undermine the Court of Appeal's thorough analysis directly refuting the core allegation underlying the Order.
[66] *Id.* at *7.
[67] *Id.* at *3–4 (emphases added).

The *Yeh* decision dismantles the factual predicate of the 2022 Order. It establishes—as a matter of adjudicated fact—that Twitter's Privacy Policy *did* disclose to users that their contact information would be used for advertising, a finding that directly contradicts the FTC complaint's core allegation that Twitter "failed to disclose" that use.[68]

The Commission has repeatedly recognized that when the factual or legal predicate of a consent order is no longer valid, the order should be modified or set aside. *See, e.g.*, *In re Agrium, Inc.*, 151 F.T.C. 658, 663 (Mar. 7, 2011) (setting aside an order in its entirety after concluding that "the fundamental premise to the Commission's Complaint . . . is now effectively a nullity"); *In re El Paso Energy Corp.*, 150 F.T.C. 839, at *4 (Oct. 4, 2010) (similar); *In re White Sands Health Care System, LLC*, No. C-4130, 2005 WL 2395787, at *3 (F.T.C. Sep. 20, 2005) (similar). Here, the FTC premised the 2022 Order on the factual allegation that Twitter deceived users by failing to disclose its use of security-purpose data for advertising. A court has now determined, on the merits and with prejudice, that this allegation was factually incorrect: the Privacy Policy did disclose that use, and users did consent to it. With the "fundamental premise" now refuted, based on the plain and express language of the Privacy Policy, allowing the Order to remain in effect for even one more day is unjustified and overreaching.

C. The Company's Total Transformation Under New Ownership Constitutes a Changed Condition of Fact.

The wholesale transformation of Twitter into X also constitutes a "changed condition[] of fact" warranting the Order's immediate termination. The entity subject to this Order is not the company that entered into it. On October 27, 2022, Elon Musk completed his acquisition of Twitter, Inc. and took it private. What followed was a root-and-branch reconstitution of the

[68] *See* Compl. ¶¶ 94, 97–98, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. May 25, 2022), Dkt. 1 (seeking civil penalties for order violations and injunctive relief, but not consumer restitution); *Yeh*, 2026 WL 44933, at *8 (finding no cognizable consumer injury).

company—its ownership, its corporate form, its leadership, its workforce, its mission, and its relationship to its users. As Twitter itself explained to the FTC during the post-acquisition period, the company was "undergoing a fundamental transformation" involving "a substantial overhaul of its organizational structure, budgeting, revenue-generation priorities, and other fundamental aspects of the business."[69] Every dimension of the company that existed when the Order was negotiated has since been replaced.

The scope of the transformation is difficult to overstate. Twitter, Inc. was merged into X Corp. on March 15, 2023, with X Corp. as the surviving entity.[70] The company was rebranded. Its corporate structure was reconstituted from the ground up. Its board of directors—which had approved the 2022 Order—was dissolved when the company went private.[71] The senior executives who had overseen the conduct giving rise to the FTC's complaint—including the Chief Privacy Officer, the Chief Information Security Officer, and the General Counsel—departed in the weeks and months following the acquisition.[72] The individuals who designed the advertising systems that improperly ingested security-purpose contact information are no longer with the company.[73] The management culture that tolerated those failures has been replaced. As described above at pp. 8–10, X has since built an entirely new privacy and information security program staffed by new personnel operating under new leadership with a fundamentally different organizational

[69] Koffmann Letter at 1.

[70] *See* Delaware Secretary of State, Certificate of Merger of X Corp. (Mar. 15, 2023), *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. Jul. 13, 2023), Dkt. 18-6.

[71] *See* Koffmann Letter at 10.

[72] *Id.* at 5, 7–9 (documenting the departures of the General Counsel, Chief Privacy Officer, and Chief Information Security Officer); Dep. of David Roque at 38:15–40:7, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. Jun. 21, 2023), Dkt. 18-14 (confirming that "a significant amount of the executives that were originally familiar with the programs" had departed, along with "the entire internal audit team . . . as well as their compliance functions").

[73] *See* Compl. ¶¶ 26–27, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. May 25, 2022), Dkt. 1; Ex. 5 to X Corp.'s Mot. for Protective Order, Dkt. 18-5 at 17.

philosophy grounded on the importance of privacy and information security being "crucial tenets of the company culture."[74]

The Commission has recognized that a company's fundamental transformation—particularly through acquisition by a new owner that reconstitutes the enterprise—is precisely the kind of changed condition that warrants reopening and setting aside an order. In *In re National Comics Publications, Inc.*, the Commission set aside orders against National Comics Publications, Inc. and Independent News Company, Inc. after those entities were acquired and fundamentally transformed—National Comics became DC Comics, a partnership between Warner Communications Inc. and Time Warner Entertainment Company, L.P., and Independent News became Warner Publisher Services, Inc.[75] The Commission found that the orders should be set aside as to the successor companies, recognizing that the corporate transformations had so altered the regulated entities that continued enforcement of the original orders against their successors was no longer warranted. The parallel to X is direct: as National Comics was to DC Comics, so Twitter is to X. The company that entered into the Order no longer exists in any meaningful sense.[76] There is no reason to continue to subject X to its terms.

II. The Public Interest Strongly Favors Setting Aside the Order.

Even if changed circumstances alone did not require setting the Order aside, the public interest would. A respondent can show that the public interest warrants termination of an order where, for example, "there is a more effective or efficient way of achieving the purposes of the order" or "the order in whole or part is no longer needed," in addition to common public interests

[74] [redacted]

[75] *In re Nat'l Comics Publ'ns, Inc.*, Docket No. 7614 (F.T.C. 1995) (setting aside orders against predecessor entities after those entities were acquired and fundamentally reconstituted under new ownership).

[76] Modifying or terminating an order is also often warranted when the company's business model has fundamentally changed, whether because of new market realities or a change in ownership. *See, e.g.*, *In re Toys "R" Us, Inc.*, 126 F.T.C. 695 (1998) (granting modification of order following fundamental changes in the toy retail market).

like avoiding harsh economic consequences, protecting innovation, or promoting American national security.[77]

Here, the public interest favors terminating the order in at least three ways. First, the Order provides vehicles for government encroachment on free expression and for efforts (like those in the last administration) to punish dissent. Second, the Order imposes a substantial burden on X that is not warranted. Third and finally, the Order hampers AI innovation, setting back core American national security priorities—interests emphasized in Executive Order 14179, "Removing Barriers to American Leadership in Artificial Intelligence."[78]

A. The Order Provides a Vehicle for Government Suppression of Free Expression.

The public interest in terminating the Order may well be at its apex here—because the Order in question functions as a loaded gun pointed at constitutionally protected expression. Simply put, the Order's sweeping investigative and enforcement powers can be deployed against X in ways untethered from their stated purpose. X is the nation's most prominent—and freest—platform for public discourse. Maintaining a sweeping consent decree over such a platform creates a standing mechanism through which a future Commission can pressure the Company over the viewpoints it hosts.

This is not a hypothetical concern. At least twice, the Biden FTC abused the Order's investigative authorities to suppress dissent and chill core First Amendment activity.

First, Commission staff invoked the Order's blanket authorization for interrogatories and document requests under Section XIII to demand detailed information about the Twitter Files project and X's relationship with various journalists. In a December 13, 2022 demand letter, FTC

[77] FTC, *Requests to Reopen*, 65 Fed. Reg. 50,636, 50,637 (Aug. 21, 2000).
[78] Exec. Order No. 14,179, 90 Fed. Reg. 8,741 (Jan. 23, 2025).

staff commanded that the Company "[i]dentify all journalists and other members of the media to whom" the Company had "granted any type of access to the Company's internal communications . . . internal documents, and/or files."[79] Staff also demanded that the Company "describe in detail . . . (ii) the purpose(s) for which such access was granted; (iii) the person(s) who made the decision to grant such access; [and] (iv) the means by which that person was granted access, including the length of time that access was granted."[80] The demand letter specifically referenced, by name, journalists Bari Weiss, Matt Taibbi, Michael Shellenberger, and Abigail Shrier—independent reporters who had been invited by Mr. Musk to review internal Twitter communications and report on what they found.[81] At no point did staff articulate a legitimate reason for these demands connected to enforcement of the Order's privacy and data protection obligations. Indeed, a legitimate purpose is difficult to conceive, raising the inference that the demands were part of an effort to intimidate the Company's new ownership to stop drawing attention to misconduct by the Biden Administration and complicit former Twitter executives, who suppressed viewpoints dissenting from the administration's COVID-19 policies.

Second, the independent assessor process established by Section VI of the Order was subjected to improper pressure by Commission staff. David Roque of Ernst & Young, Twitter's independent assessor, later testified that he "felt as if the FTC was trying to influence the outcome of the engagement before it had started" and that the FTC conveyed its expectation that EY "would conclude that there were deficiencies in Twitter's privacy and information security program."[82]

---

[79] Letter from Reenah L. Kim, FTC, to Robert A. Zink & Daniel Koffmann, Quinn Emanuel, at 1–2, Ex. 9 to X Corp.'s Mot. for Protective Order, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH, Dkt. 18-9 (N.D. Cal. Jul. 13, 2023).

[80] *Id.* at 2.

[81] *Id.* at 1.

[82] Dep. of David Roque at 120:20–22, 199:6–200:12, *United States v. Twitter, Inc.*, No. 3:22-cv-03070-TSH (N.D. Cal. Jun. 21, 2023), Dkt. 18-14; *see also id.* at 124:14–21.

He further testified that the FTC gave EY "a list of specific[] . . . types of procedures they were expecting us to execute" and told him that if EY's report "didn't have [certain] findings," EY "should expect the FTC would follow up very significantly."[83] The FTC's conduct made a mockery of the principle that independent assessors be truly independent and objective. These incidents illustrate how the Order's expansive investigative authorities can be weaponized against core First Amendment activity. As the Supreme Court recognized in *Moody v. NetChoice, LLC*, 603 U.S. 707 (2024), social media platforms engage in constitutionally protected editorial discretion and content-moderation decisions. Maintaining a sweeping consent decree with standing subpoena-like powers over such a platform creates precisely the kind of ongoing coercive pressure that risks chilling the marketplace of ideas. As long as the Order remains in force, the same tools that enabled past abuses remain available to any future official inclined to use them. Consent orders cannot be judged on the assumption of prudent enforcement, but on the reality that their powers may be exercised by officials with very different aims. An order that is sound only in the hands of the exceptionally restrained is not sound at all.

Given the public's interest in a free public square and a robust First Amendment interest, the Order should be terminated as unsound and prone to abuse. Freedom of speech is a foundational constitutional commitment that must inform every exercise of the Commission's authority. As Chairman Ferguson has emphasized, "freedom of speech—which makes the marketplace of ideas possible—is a value deeply woven into the very fabric of our constitutional order and our society."[84] Further, the Chairman has rightly warned of the danger that "government officials backed with potential coercive power—formal and informal" will pressure platforms to proscribe

[83] *Id.* at 201:13–15, 124:14–21.

[84] FTC, *Andrew N. Ferguson, Chairman, FTC, Keynote Address at the Stigler Center Antitrust and Competition Conference* (Apr. 10, 2025), https://www.promarket.org/2025/04/17/transcript-ftc-chair-andrew-ferguson-keynote/

disfavored ideas.[85] Consent decrees are a quintessential source of such coercive power. The Commission has thus long recognized that consent orders must avoid chilling the exercise of First Amendment rights, and has reopened and modified consent orders to uphold that requirement.[86]

The Commission should do so again. The Order's tools are not merely susceptible to speech-chilling misuse; they have actually been deployed to that end. The Order should be terminated so that the most significant platform for open public discourse in the digital age is not perpetually subject to the threat that a future regulator will convert a privacy decree into an instrument of censorship.

D. The Order Imposes Substantial and Unwarranted Burdens on the Company.

It is well established that the public interest favors the elimination of order provisions that impose substantial and unwarranted burdens on private companies without corresponding consumer benefit. The Commission has repeatedly recognized this principle. For instance, in *Reader's Digest*, the Commission reopened and set aside an order provision after concluding that "the costs that the absolute ban . . . imposes on respondent appear to outweigh any consumer benefits the ban may confer," and that "the public interest requires eliminating" the offending provision.[87] The Commission's 2000 policy statement on order modification further confirmed that the public interest standard is met when a respondent demonstrates "that there is a more effective or efficient way of achieving the purposes of the order" or "that the order in whole or

[85] FTC, *Andrew N. Ferguson, Chairman, FTC, Keynote Address at the Stigler Center Antitrust and Competition Conference: Audience Q&A* (Apr. 10, 2025), https://www.promarket.org/2025/04/21/transcript-ftc-chairman-andrew-ferguson-keynote-part-ii/.

[86] *E.g.*, *In re Am. Coll. of Obstetricians and Gynecologists*, 104 F.T.C. 524, 526 (1984) (reopening and modifying consent order to eliminate provisions that improperly restricted constitutionally protected speech).

[87] *In re Reader's Dig. Ass'n*, 102 F.T.C. 1268, 1290 (1983).

part is no longer needed."[88] Similarly, the Commission has emphasized that the modification process exists to "keep Commission orders from doing more harm than good."[89]

The 2022 Order imposes ongoing obligations that add paperwork and other burdens on top of the company's existing legal obligations—consuming enormous resources for the Company and for the Commission itself. Section V requires the Company to document a comprehensive privacy and information security program; conduct annual risk assessments; maintain annual training programs; designate a senior officer for data-use decisions; and evaluate the program annually.[90] Section VI requires biennial independent assessments covering [redacted] across twenty-four domains.[91] Section VIII, XI, and XII layer on additional annual certifications, compliance reports, and expansive recordkeeping requirements spanning twenty years.

The practical cost of these requirements is staggering. Since 2022, the Company has expended nearly $17 million and thousands of hours of personnel time responding to the FTC's enforcement of the Order.[92] By mid-2023—less than a year into the Order's term—X Corp. had responded to more than 200 demands for information and documents and produced more than 22,000 documents to the Commission, at a pace of approximately one new demand letter every two weeks.[93] The cost of engaging an independent assessor to evaluate [redacted] is also substantial, requiring months of intensive auditor review, hundreds of interviews and evidence

[88] FTC, *Requests to Reopen*, 65 Fed. Reg. at 50,637.

[89] FTC, *Putting the "Mod" in Order Modification* (July 17, 2014), https://www.ftc.gov/enforcement/competition-matters/2014/07/putting-mod-order-modification.

[90] 2022 Order §§ V.A–I.

[91] *Id.* §§ VI.A–E; [redacted]

[92] *See* Ex. C, Harris Decl. ¶¶ 4–5.

[93] *See* Koffmann Letter at 1–2 (describing twenty-seven requests with more than 100 subparts in a single demand letter and noting the Company's resource constraints in responding); *see also* Dkt. 18, Exs. 1–13 (attaching representative demand letters spanning August 2022 to May 2023).

requests, and the production of assessment reports spanning hundreds of pages—not to mention all the employee hours redirected toward facilitating the assessment.[94]

These costs fall not only on the Company but also on the Commission, whose staff must review, process, and follow up on each submission—diverting scarce agency resources from investigating genuinely harmful practices elsewhere in the marketplace. Those burdens might be tolerable if they produced marginal consumer-protection benefits commensurate with their cost. They do not. As demonstrated in Section I.A above, the Order has already achieved its purpose, and significant privacy and information security safeguards do not depend on its continuance. The Company will maintain robust data-protection safeguards regardless of the Order's existence.[95] What the Order adds, at this point, is not protection but paperwork. Because the burdens it continues to impose are not justified, the Order should now be set aside without delay.[96]

At a minimum, the Order should be modified with a new termination date on or before December 31, 2026. If it is not set aside before 2027, X Corp. will need to take costly steps toward completing another unnecessary and burdensome biennial assessment.[97]

E. The Order Harms American AI Innovation.

The public has a profound interest in American leadership in artificial intelligence. AI is among the most consequential technologies in human history—a tool of extraordinary promise that stands to transform medicine, scientific research, education, communication, and economic

---

[94] *See* Harris Decl. ¶¶ 4–5; [redacted]

[95] *See supra* Part II.B.

[96] Recent commentary has highlighted the broader public-interest costs of the FTC's longstanding 20-year consent-order policy, which imposes perpetual or near-perpetual burdens long after any remedial purpose has been served. Terminating this Order would align with calls to modernize that policy and avoid unnecessary regulatory overhang on transformed companies. *See, e.g.*, John Villafranco & Andrea deLorimier, *FTC Consumer Protection Orders: The Case for a New Sunset Policy*, Wash. Legal Found. (May 30, 2025), https://www.wlf.org/2025/05/30/publishing/ftc-consumer-protection-orders-the-case-for-a-new-sunset-policy/ (explaining that 20-year and indefinite order terms "are simply not sensible or desirable" because they are unduly burdensome, inconsistent with other agencies' practices, and hinder innovation).

[97] 2022 Order § VI(C)–(E).

productivity in ways that will improve the lives of hundreds of millions of people. But the public interest in AI extends beyond the domestic benefits of innovation. It is now a core national-security imperative that the United States prevail in the global competition for AI supremacy.

As President Trump recognized in Executive Order 14179, "Removing Barriers to American Leadership in Artificial Intelligence" (Jan. 23, 2025), the United States must "sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security."[98] The White House's subsequent AI Action Plan, "Winning the Race" (July 2025), was even more explicit: "Whoever has the largest AI ecosystem will set global AI standards and reap broad economic and military benefits. Just like we won the space race, it is imperative that the United States and its allies win this race."[99] These concrete directives are grounded in the recognition that the People's Republic of China is investing vast resources in AI with the explicit aim of surpassing the United States, and that losing this race would have profound consequences for American security and the free world.

The current Administration and this Commission have acted on that imperative. In January 2025, the President revoked the prior administration's AI executive order, which had "impos[ed] burdensome government requirements restricting private sector AI development and deployment," and directed the creation of an AI Action Plan to chart a course for American dominance.[100] The AI Action Plan, released in July 2025, specifically instructs the Commission to "review all FTC final orders, consent decrees, and injunctions, and, where appropriate, seek to modify or set-aside any that unduly burden AI innovation."[101] The Commission has already begun acting on this

[98] Exec. Order No. 14,179, 90 Fed. Reg. at 8,741.
[99] *Winning the Race: America's AI Action Plan* at 1.
[100] Exec. Order No. 14,179, 90 Fed. Reg. at 8,741.
[101] *Winning the Race: America's AI Action Plan* at 3–4.

directive. In *In the Matter of Rytr LLC*, the Commission reopened and set aside a consent order that had banned an AI-enabled writing service, concluding that "the Order unduly burdens innovation in the nascent AI industry" and that "[r]ushing in to impose aggressive law enforcement unsupported by facts or law is improper and is not in the public interest."[102]

The same analysis applies with even greater force here. Terminating the Order directly advances the cause of American AI innovation. X today operates at the center of a family of companies—including xAI, the developer of the Grok large language model, and SpaceX—that are at the forefront of artificial intelligence, aerospace, and related frontier technologies. These entities are central to America's technological leadership. As X has explained, the Order imposes a regulatory apparatus that diverts critical engineering resources from innovation to compliance paperwork, introduces friction into product development where speed and agility are essential, and creates an overhang of regulatory uncertainty that chills experimentation.[103] This is precisely the kind of outdated encumbrance that President Trump's Executive Order 14179 and subsequent AI Action Plan were designed to address. Every hour that X's engineers spend preparing for biennial assessments, responding to demand letters, or documenting privacy reviews for features that are already governed by other legal regimes is an hour not spent building AI tools that serve users and advance American competitiveness. The Order's mandatory independent assessment process alone requires months of review, hundreds of interviews, and assessment reports spanning hundreds of pages, consuming resources that could otherwise be devoted to research and development.[104]

---

[102] Order Reopening and Setting Aside Order at 6, *In re Rytr LLC*, Docket No. C-4806 (F.T.C. Jan. 23, 2025).

[103] *See* Section II.A, *supra* (cataloguing the Order's compliance burdens).

[104] Moreover, just as the Order's enforcement tools create a risk that a future Commission hostile to free speech could use the Order as leverage, those same tools create a risk that a future Commission hostile to X's technological choices could use the decree as leverage. That leverage would be over not just X, but the whole family of companies.

Simply put, "AI is far too important to smother in bureaucracy at this early stage."[105] Every unnecessary regulatory burden imposed through the Order diverts resources and attention from developing technologies that are critical to winning the global AI race. Every day it is in effect is a day where American AI is not allowed to reach its full potential. The Commission should heed the President's directive and set aside the Order so that one of America's most important technology companies can devote its full energies to the innovation that the Nation's security and prosperity demand.

CONCLUSION

Fifteen years of onerous regulatory oversight is enough. Respondent respectfully requests that the Commission promptly reopen these proceedings and set aside the Order in its entirety. Alternatively, Respondent requests that the Commission reopen these proceedings and modify the Order to terminate on or before December 31, 2026.

Dated: May 15, 2026

Respectfully submitted,

By: /s/ William R. Levi

William R. Levi
Manuel Valle
Sidley Austin LLP
1501 K Street, N.W.
Washington, DC 20005
Telephone: (202) 736-8546
Fax: (202) 736-8000
william.levi@sidley.com
manuel.valle@sidley.com
Counsel for Respondent

[105] *Winning the Race: America's AI Action Plan* at 3.

EXHIBIT A

202-3062

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Noah Joshua Phillips
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of	**DECISION AND ORDER**
TWITTER, INC., *a corporation.*	**Docket No. C-4316**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. BCP proposed presenting the draft Complaint to the Commission. If issued, the draft Complaint would charge Respondent with violations of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(a)(1) and (*l*), 53(b), and 56(a)(1).

Respondent neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Respondent admits the facts necessary to establish jurisdiction.

The Commission considered the matter and determined that it had reason to believe Respondent has violated the Decision and Order the Commission previously issued in *In re Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. March 2, 2011) and the FTC Act, and that a Complaint should issue stating its charges in that respect. After due consideration, the Commission issues the Complaint, makes the following Findings, and issues the following Order:

FINDINGS

1. Respondent Twitter, Inc. ("Twitter") is a Delaware corporation with its principal office or place of business at 1355 Market Street, Suite 900, San Francisco, CA 94103.

2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

3. The Complaint charges violations of Section 5 of the FTC Act, 15 U.S.C. § 45, and violations of Provision I of an order previously issued by the Commission, 15 U.S.C. § 56(a)(1).

4. Respondent waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorney fees.

5. Respondent and the Commission waive all rights to appeal or otherwise challenge or contest the validity of this Order.

ORDER

DEFINITIONS

For the purpose of this Order, the following definitions apply:

A. "**Covered Incident**" means any instance affecting 250 or more Users in which: (1) any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization; or (2) individually identifiable Covered Information collected or received, directly or indirectly, by Respondent, was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization. "Covered Incident" does not include instances where the only unauthorized access, acquisition, or exposure was due to a User communicating through Respondent's services (e.g., public tweets, protected tweets, retweets, or direct messages) information that was obtained from sources other than Respondent.

B. "**Covered Information**" means information from or about an individual consumer including, but not limited to: (1) a first or last name; (2) geolocation information sufficient to identify a street name and name of city or town; (3) an email address or other online contact information, such as an instant messaging User identifier or a screen name; (4) a mobile or other telephone number; (5) photos and videos; (6) Internet Protocol ("IP") address, User ID, or other persistent identifier that can be used to recognize a User over time and across different devices, websites, or online services; (7) a Social Security number; (8) a driver's license or other government issued identification number; (9) financial account number; (10) credit or debit information; (11) date of birth; (12) biometric information; or (13) any information combined with any of (1) through (12) above. "Covered Information" does not include information that a User intends to make public using Respondent's services.

C. "**Representatives**" means Respondent's officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.

D. "**Resources**" means networks, systems, and software.

E. "**Respondent**" means Twitter, Inc. ("Twitter"), and its successors and assigns. For purposes of Parts V and VI, Respondent means Twitter, Inc., its successors and assigns, and any business that Respondent controls directly or indirectly, except for any business that: (1) does not provide services that are offered to U.S. residents; or (2) does not collect, maintain, use, disclose,

access, or provide access to the Covered Information of U.S. residents to enable Respondent's microblogging, social networking, or communications services.

F. "**Timeline Notice**" means a message Respondent places in a User's Twitter timeline (*i.e.*, the main screen the User sees when opening Twitter which displays a stream of tweets from accounts the User has chosen to follow) that stays near the top (*i.e.*, within the first five (5) tweets) of a User's Twitter timeline: (1) for at least six (6) months from the effective date of the Order; (2) until the User clicks on the "Learn More about your options" button embedded in the message; or (3) until the User scrolls past the message in their timeline, whichever occurs earlier.

G. "**User**" means an identified individual from whom Respondent has obtained information for the purpose of providing access to Respondent's products and services.

I. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS ORDERED that Respondent and its Representatives, directly or through any corporation, subsidiary, division, website, mobile app, or other device, in connection with the offering of any product or service in or affecting commerce, must not misrepresent, in any manner, expressly or by implication, the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, misrepresentations related to:

A. Respondent's privacy and security measures to prevent unauthorized access to Covered Information;

B. Respondent's privacy and security measures to honor the privacy choices exercised by Users;

C. Respondent's collection, maintenance, use, disclosure, or deletion of Covered Information;

D. The extent to which a User can control the privacy of any Covered Information maintained by Respondent, and the steps a User must take to implement such controls;

E. The extent to which Respondent makes or has made Covered Information accessible to any third parties;

F. The extent to which Respondent targets advertisements to Users or enables third parties to target advertisements to Users; or

G. The extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules.

II. LIMITATIONS ON USE OF TELEPHONE NUMBERS OR EMAIL ADDRESSES SPECIFICALLY PROVIDED TO ENABLE ACCOUNT SECURITY FEATURES

IT IS FURTHER ORDERED that Respondent and its Representatives must not use, provide access to, or disclose, for the purpose of serving advertisements, any telephone number or email address obtained from a User before the effective date of this Order for the purpose of enabling an account security feature (*e.g.*, two-factor authentication, password recovery, re-authentication after detection of suspicious or malicious activity). Nothing in Provision II will limit Respondent's ability to use, provide access to, or disclose such telephone numbers or email addresses if obtained separate and apart from a User enabling such account security feature and in a manner consistent with the requirements of this Order.

III. REQUIRED NOTICE TO CONSUMERS

IT IS FURTHER ORDERED that, within fourteen (14) days after the effective date of this Order, Respondent must provide a Timeline Notice to all current U.S. Users who joined Twitter prior to September 17, 2019, that states: "**Twitter's Use of Your Personal Information for Tailored Advertising** As we stated on Oct. 8, 2019, we may have served you targeted ads based on an email address or phone number you provided to us to secure your account.", and includes a "Learn more about your options" button that links to a webpage showing the information in Exhibit A.

IV. REQUIRED MULTI-FACTOR AUTHENTICATION OPTIONS

IT IS FURTHER ORDERED that, as of the effective date of this Order, Respondent must allow Users to utilize multi-factor authentication without providing a telephone number to access their Twitter accounts, such as by integrating authentication applications or allowing the use of security keys. The Company may use equivalent, widely-adopted industry authentication options that do not require Users to provide a telephone number and that are not multi-factor, if the person or persons responsible for the Program under Provision V.C: (1) approve(s) in writing the use of such equivalent authentication options; and (2) document(s) a written explanation of how the authentication options are widely-adopted and at least equivalent to the security provided by multi-factor authentication.

V. MANDATED PRIVACY AND INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Respondent, in connection with the collection, maintenance, use, disclosure of, or provision of access to Covered Information, must, within one hundred eighty (180) days of issuance of this Order, establish and implement, and thereafter maintain a comprehensive privacy and information security program (the "Program") that protects the privacy, security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, Respondent must at a minimum:

A. Document in writing the content, implementation, and maintenance of the Program;

B. Provide the written program, and any evaluations thereof or updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent governing

body exists, to a senior officer of Respondent responsible for the Program at least once every calendar quarter;

C. Designate a qualified employee or employees to coordinate and be responsible for the Program;

D. Assess and document, at least once every twelve (12) months and promptly following the resolution of a Covered Incident (not to exceed ninety 90 days after the discovery of the Covered Incident), internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information that could result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information;

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Respondent identifies to the privacy, security, confidentiality, or integrity of Covered Information identified in response to Provision V.D. Each safeguard must be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized and result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, or destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information. Such safeguards must also include:

1. Prior to implementing any new or modified product, service, or practice that collects, maintains, uses, discloses, or provides access to Covered Information, conducting an assessment of the risks to the privacy, security, confidentiality, or integrity of the Covered Information;

2. For each new or modified product, service, or practice that does not pose a material risk to the privacy, security, confidentiality, or integrity of Covered Information, documenting a description of each reviewed product, service, or practice and why such product, service, or practice does not pose such a material risk;

3. For each new or modified product, service, or practice that poses a material risk to the privacy, security, confidentiality, or integrity of Covered Information, conducting a privacy review and producing a written report ("Privacy Review") for each such new or modified product, service, or practice. The Privacy Review must:

(a) Describe how the product, service, or practice will collect, maintain, use, disclose, or provide access to Covered Information, and for how long;

(b) Identify and describe the types of Covered Information the product, service, or practice will collect, maintain, use, disclose, or provide access to;

(c) If the Covered Information will be collected from a User, describe the context of the interaction in which Respondent will collect such Covered Information (*e.g.*, under security settings, in pop-up messages in the timeline, or in response to a prompt reading, "Get Better Ads!");

(d) Describe any notice that Respondent will provide Users about the collection, maintenance, use, disclosure, or provision of access to the Covered Information;

(e) State whether and how Respondent will obtain consent from Users for the collection, maintenance, use, disclosure, or provision of access to Covered Information;

(f) Identify any privacy controls that will be provided to Users relevant to the collection, maintenance, use, disclosure, or provision of access to the Covered Information;

(g) Identify any third parties to whom Respondent will disclose or provide access to the Covered Information;

(h) Assess and describe the material risks to the privacy, security, confidentiality, and integrity of Covered Information presented by the product, service, or practice;

(i) Assess and describe the safeguards to control for the identified risks, and whether any additional safeguards need to be implemented to control for such risks;

(j) Explain the reasons why Respondent deems the notice and consent mechanisms described in Provisions V.E.3(d) and V.E.3(e) sufficient;

(k) Identify and describe any limitations on the collection, maintenance, use, disclosure, or provision of access to Covered Information based on: (i) the context of the collection of such Covered Information; (ii) notice to Users; and (iii) any consent given by Users at the time of collection or through subsequent authorization;

(l) Identify and describe any changes in how privacy and security-related options will be presented to Users, and describe the means and results of any testing Respondent performed in considering such changes, including but not limited to A/B testing, engagement optimization, or other testing to evaluate a User's movement through a privacy or security-related pathway;

(m) Include any other safeguards or other procedures that would mitigate the identified risks to the privacy, security, confidentiality, and integrity of Covered Information that were not implemented, and each reason that such alternatives were not implemented; and

(n) Include any decision or recommendation made as a result of the review (*e.g.*, whether the practice was approved, approved contingent upon safeguards or other recommendations being implemented, or rejected);

4. Safeguards to prevent the collection, maintenance, use, disclosure, or access to Covered Information beyond the limitations identified in Provision V.E.3(k), including:

(a) Regular training, at least once a year, for any employees and independent contractors whose responsibilities include the collection, maintenance, disclosure, use, or provision of access to Covered Information, on the permissible collection, maintenance, disclosure, use, or provision of access to Covered Information and any related limitations;

(b) Written attestations by those employees and independent contractors that they will not collect, maintain, disclose, use, or provide access to the Covered Information in a manner inconsistent with those limitations;

(c) Designation of a senior officer, or senior level team composed of no more than five (5) persons, to be responsible for any decision to collect, maintain, use, disclose, or provide access to the Covered Information; and

(d) Treating any new method of collecting, maintaining, using, disclosing, providing access to, or deleting the Covered Information as a new or modified product, service, or practice requiring the reviews set forth in Provisions V.E.1-3;

5. Regular privacy and information security training programs for all employees and independent contractors on at least an annual basis, updated to address any identified material internal or external risks and safeguards implemented pursuant to this Order;

6. Technical measures to monitor Respondent's Resources to identify unauthorized attempts to: (a) access, modify, or exfiltrate Covered Information from Respondent's Resources; or (b) access or take over Users' accounts; and

7. Data access policies and controls for all: (a) databases storing Covered Information; (b) Resources that provide access to Users' accounts; and (c) Resources containing information that enables or facilitates access to Respondent's internal network and systems;

F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information, and modify the Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, and modify the Program based on the results. Such testing and monitoring must include: (1) vulnerability testing of Respondent's network(s) once every four (4) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources; and (2) penetration testing of Respondent's network(s) at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources;

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information; and

I. Evaluate and adjust the Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision V.D of this Order, or any other circumstances that Respondent knows or has reason to believe may have an impact on the effectiveness of the Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Program at least once every twelve (12) months and modify the Program based on the results.

VI. INDEPENDENT PROGRAM ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Provision V of this Order titled Mandated Privacy and Information Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from one or more qualified, objective, independent third-party professionals ("Assessor(s)") who: (1) use procedures and standards generally accepted in the profession; (2) conduct an independent review of the Program; (3) retain all documents relevant to each Assessment for five (5) years after completion of such Assessment; and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents relating to Respondent's compliance with this Order may be withheld from the Commission by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim. Respondent may obtain separate assessments for (1) privacy and (2) information security from multiple Assessors, so long as each of the Assessors meets the qualifications set forth above;

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion;

C. The reporting period for the Assessments must cover: (1) the first three-hundred-and-sixty-five (365) days after the issuance date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments;

D. Each Assessment must, for the entire assessment period: (1) determine whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy and Information Security Program; (2) assess the effectiveness of Respondent's implementation and maintenance of Provisions V.A-I; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Program that were

identified in any prior Assessment required by this Order; and (5) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is: (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Program and did not rely primarily on assertions or attestations by Respondent's management. To the extent that Respondent revises, updates, or adds one or more safeguards required under Provision V.E of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard; and

E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Twitter, Inc., FTC File No. 202-3062." All subsequent biennial Assessments must be retained by Respondent until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

VII. COOPERATION WITH THIRD-PARTY ASSESSOR(S)

IT IS FURTHER ORDERED that Respondent and its Representatives, whether acting directly or indirectly, in connection with any Assessment required by Provision VI of this Order titled Independent Program Assessments by a Third Party, must:

A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the Assessor information about Respondent's Resources(s) and all of Respondent's IT assets so that the Assessor can determine the scope of the Assessment, and have visibility to Resource(s) and IT assets deemed in scope; and

C. Disclose all material facts to the Assessor(s), and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy and Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of Provisions V.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Program.

VIII. CERTIFICATIONS

IT IS FURTHER ORDERED that Respondent must:

A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for the Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification; and

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Twitter, Inc., FTC File No. 202-3062."

IX. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondent, within thirty (30) days after Respondent's discovery of a Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;

C. A description of each type of Covered Information that was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;

D. The number of Users whose Covered Information was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;

E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

F. A representative copy of any materially different notice sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW,

Washington, DC 20580. The subject line must begin, "*In re Twitter, Inc.*, FTC File No. 202-3062."

X. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For five (5) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities relating to the subject matter of this Order, and all agents and representatives who participate in any acts or practices subject to this Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order, which can be obtained electronically.

XI. COMPLIANCE REPORTING AND NOTICES

IT IS FURTHER ORDERED that Respondent makes timely submissions to the Commission:

A. Two-hundred and forty (240) days after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent: (1) identifies the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (2) identifies all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describes the activities of each business, including the goods and services offered and the means of advertising, marketing, and sales; (4) describes in detail whether and how Respondent is in compliance with each Provision of this Order; and (5) provides a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; (3) the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent.

C. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

D. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Twitter, Inc., FTC File No. 202-3062."

XII. RECORDKEEPING

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each person that Respondent contracts with directly and that provides services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Copies or records of all U.S. consumer complaints concerning the subject matter of the Order, and any responses to such complaints;

D. A copy of each unique advertisement or other marketing material making a representation subject to this Order;

E. A copy of each widely-disseminated representation by Respondent or its Representatives that describe the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, (1) statements relating to any change in any product, service, or practice that relates to the privacy, security, confidentiality, or integrity of such information, and (2) statements relating to: (a) Respondent's privacy and security measures to prevent unauthorized access to Covered Information; (b) Respondent's privacy and security measures to honor the privacy choices exercised by Users; (c) Respondent's collection, maintenance, use, disclosure, or deletion of Covered Information; (d) the extent to which a User can control the privacy of any Covered Information maintained by Respondent, and the steps a User must take to implement such controls; (e) the extent to which Respondent makes or has made Covered Information accessible to any third parties; (f) the extent to which Respondent allows third parties to serve advertisements to Users; or (g) the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules;

F. All materials relied upon in making the statements in Provisions XII.D and XII.E, and copies of each materially different notice provided to Users and mechanisms for obtaining a User's consent for the collection, use, or disclosure of Covered Information (including screenshots/screencasts and User interfaces, consent flows, and paths a User must take to reach such settings);

G. All materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

H. For 5 years from the date received, copies of all subpoenas, information provided in response to such subpoenas, and all material correspondence with law enforcement, if such communication relate to Respondent's compliance with this Order;

I. For 5 years from the date created or received, all records, whether prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this Order; and

J. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

XIII. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within fourteen (14) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce records for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIV. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than twenty (20) years;

B. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED: May 26, 2022

EXHIBIT B

Petitioner has requested confidential treatment of the entirety of this exhibit pursuant to FOIA Exemption 4, 5 U.S.C. § 552(b)(4), the FTC Act, 15 U.S.C. § 46(f), 16 C.F.R. § 4.10(a)(2), and all other applicable statues, regulations, and confidentiality policies.

EXHIBIT C

PUBLIC

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Andrew N. Ferguson, Chair**
Mark Meador

In the Matter of **Twitter, Inc.** **a corporation;**	**Docket No. C-4316**

Declaration of Joshua Harris in support of Petition of X Corp. to Reopen and Set Aside Decision and Order

I, Joshua Harris, declare as follows:

1. I am Global Data Protection Officer and Head of Privacy at X Corp.

2. I have been employed at X Corp. since September 2022.

3. In my role at X Corp., I have personal knowledge of the expenditures and reallocation of employee time that has been made necessary by the Commission's Decision and Order ("Order") entered on May 26, 2022 in the above-captioned proceeding.

4. Since 2022, X Corp. has spent approximately $15.6 million on legal fees and auditor fees to comply with the Order.

5. In addition, X Corp. has dedicated approximately 13,000 staff hours to work required by the Order, including facilitating risk assessments and responding to specific demands made by the Commission pursuant to Section 13 of the Order. Those staff hours can be valued at approximately $1 million.

I declare the foregoing is true and correct to the best of my knowledge and belief.

/s/ Joshua Harris

Joshua Harris

PUBLIC

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Andrew N. Ferguson, Chair**
Mark Meador

In the Matter of **Twitter, Inc.** **a corporation;**	**Docket No. C-4316**

NOTICE OF APPEARANCE OF WILLIAM R. LEVI

Pursuant to 16 C.F.R. § 4.1(d), I, William R. Levi, submit my notice of appearance on behalf of Respondent X Corp. in Docket Number C-4316. I am qualified pursuant to § 4.1(a)(1)(i) because I am admitted to the highest court of the District of Columbia (Bar No. 1007057) as well as the U.S. Supreme Court, the U.S. Courts of Appeals for the 2nd, 3rd, 5th, 6th, 7th, 9th, 10th, D.C., and Federal Circuits, the U.S. District Court for the District of Columbia, and the U.S. Court of Federal Claims. I attest to my good standing within the legal profession.

Dated: May 15, 2026

Respectfully submitted,

By: /s/ William R. Levi
William R. Levi

PUBLIC

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Andrew N. Ferguson, Chair**
Mark Meador

In the Matter of **Twitter, Inc.** **a corporation;**	**Docket No. C-4316**

NOTICE OF APPEARANCE OF MANUEL VALLE

Pursuant to 16 C.F.R. § 4.1(d), I, Manuel Valle, submit my notice of appearance on behalf of Respondent X Corp. in Docket Number C-4316. I am qualified pursuant to § 4.1(a)(1)(i) because I am admitted to the highest courts of the District of Columbia (Bar No. 1697419) and Michigan (Bar No. P82585). I attest to my good standing within the legal profession.

Dated: May 15, 2026

Respectfully submitted,

By: /s/ Manuel Valle
Manuel Valle