

1 BRIAN M. BOYNTON, Principal Deputy Assistant Attorney General
ARUN G. RAO, Deputy Assistant Attorney General
2 GUSTAV W. EYLER, Director
LISA K. HSIAO, Assistant Director
3 ZACHARY L. COWAN, Trial Attorney (NCBN 53432)
4 DEBORAH S. SOHN, Trial Attorney (NYBN 5118096, DCBN 1025098)

5 U.S. Department of Justice
Civil Division
6 Consumer Protection Branch
450 5th Street NW, Suite 6400-S
7 Washington, DC 20530
8 Telephone: (202) 451-7468
Zachary.L.Cowan@usdoj.gov
9 Deborah.S.Sohn@usdoj.gov

10 STEPHANIE M. HINDS, United States Attorney (CABN 154284)
11 MICHELLE LO, Chief, Civil Division (NYBN 4325163)
SHARANYA MOHAN, Assistant United States Attorney (NYBN 5027768)
12 EMMET P. ONG, Assistant United States Attorney (NYBN 4581369)

13 Northern District of California
450 Golden Gate Avenue
14 San Francisco, California 94102
15 Telephone: (415) 436-7198
sharanya.mohan@usdoj.gov
16 emmet.ong@usdoj.gov

17 Attorneys for Plaintiff
18 UNITED STATES OF AMERICA

19 **UNITED STATES DISTRICT COURT**
NORTHERN DISTRICT OF CALIFORNIA

20
21 UNITED STATES OF AMERICA,
22
23 Plaintiff,
24 v.
25 TWITTER, INC., a corporation,
26 Defendant.
27

Case No. 3:22-cv-3070

**COMPLAINT FOR CIVIL
PENALTIES, PERMANENT
INJUNCTION, MONETARY
RELIEF, AND OTHER
EQUITABLE RELIEF**

1 Plaintiff, the United States of America, acting upon notification and authorization to the Attorney
2 General by the Federal Trade Commission (“FTC” or “Commission”), for its Complaint alleges:

3 1. Plaintiff brings this action against Defendant Twitter, Inc. (“Twitter”) under Section
4 16(a)(1) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 56(a)(1), which authorizes
5 Plaintiff to seek, and the Court to order, permanent injunctive relief, monetary relief, civil penalties, and
6 other equitable relief for Twitter’s acts or practices in violation of Section 5(a) of the FTC Act,
7 15 U.S.C. § 45(a), and a 2011 order previously issued by the FTC for alleged violations of Section 5(a)
8 of the FTC Act. *See* Exhibit A, *In re Twitter, Inc.*, C-4316, 151 F.T.C. 162 (Mar. 11, 2011) (Decision
9 and Order) (“Commission Order” or “2011 Order”).

10 2. From at least May 2013 until at least September 2019, Twitter misrepresented to users of
11 its online communication service the extent to which it maintained and protected the security and
12 privacy of their nonpublic contact information. Specifically, while Twitter represented to users that it
13 collected their telephone numbers and email addresses to secure their accounts, Twitter failed to disclose
14 that it also used user contact information to aid advertisers in reaching their preferred audiences.
15 Twitter’s misrepresentations violate the FTC Act and the 2011 Order, which specifically prohibits the
16 company from making misrepresentations regarding the security of nonpublic consumer information.
17 Plaintiff therefore seeks civil penalties for Twitter’s violations, as well as a permanent injunction and
18 other equitable relief, to ensure Twitter’s future compliance with the law.

19 **JURISDICTION, VENUE, AND DIVISIONAL ASSIGNMENT**

20 3. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331,
21 1337(a), 1345, and 1355, and 15 U.S.C. § 56(*l*), because it involves claims arising under federal laws
22 regulating commerce and is commenced by the United States of America.

23 4. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(1), (b)(2), (c)(2), (d), and
24 1395(a), as well as 15 U.S.C. § 53(b), because Twitter has its principal place of business in this District,
25 because Twitter transacts business in this District, and because a substantial part of the events or
26 omissions giving rise to the claims occurred in this District.

1 5. Divisional assignment to the San Francisco or Oakland Division is proper under Local
2 Rule 3-2(c) and (d) because Twitter has its principal place of business in San Francisco and because a
3 substantial part of the events or omissions giving rise to the claims occurred there.

4 **PLAINTIFF**

5 6. Plaintiff, the United States of America, brings this action under Sections 5(a) and (l),
6 13(b), and 16(a)(1) of the FTC Act, 15 U.S.C. §§ 45(a) and (l), 53(b), and 56(a)(1), which prohibit
7 unfair or deceptive acts or practices in or affecting commerce, and the 2011 Order.

8 **DEFENDANT**

9 7. Twitter is a Delaware corporation with its principal place of business at 1355 Market
10 Street, Suite 900, San Francisco, California, 94103. Twitter transacts or has transacted business in this
11 District and throughout the United States. At all times material to this Complaint, Twitter has operated
12 its online communication service through its website, www.twitter.com, and through its mobile
13 applications.

14 **COMMERCE**

15 8. At all times relevant to this Complaint, Twitter has maintained a substantial course of
16 trade in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

17 **THE FTC ACT**

18 9. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits “unfair or deceptive acts or
19 practices in or affecting commerce.”

20 10. Acts or practices are unfair under Section 5(a) of the FTC Act if they cause or are likely
21 to cause substantial injury to consumers that those consumers cannot reasonably avoid themselves and
22 that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

23 11. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or
24 practices prohibited by Section 5(a) of the FTC Act.

25 12. Section 5(l) of the FTC Act, 15 U.S.C. § 45(l), declares that “[a]ny person, partnership, or
26 corporation who violates an order of the Commission after it has become final, and while such order is
27 in effect, shall forfeit and pay to the United States a civil penalty[.]”

THE COMMISSION ORDER

1
2 13. In the Commission’s 2011 Administrative Complaint in the proceeding bearing Docket
3 No. C-4316 (the “Administrative Complaint”), the Commission charged Twitter with engaging in
4 deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), for its failures
5 to provide reasonable security measures to prevent unauthorized access to nonpublic user information
6 and to honor the privacy choices exercised by Twitter users.

7 14. Specifically, the Administrative Complaint asserted that Twitter had engaged in
8 deceptive acts or practices by misrepresenting that users could control who had access to their tweets
9 through a “protected account” or could send private “direct messages” that could only be viewed by the
10 recipient when, in fact, Twitter lacked reasonable safeguards to ensure those choices were honored, such
11 as restricting employee access to nonpublic user information based on a person’s job requirements.

12 15. The Administrative Complaint also alleged that Twitter had misrepresented the controls it
13 implemented to keep user accounts secure, when, in fact, Twitter lacked reasonable safeguards to limit
14 or prevent unauthorized access to nonpublic user information, such as secure password requirements and
15 other administrative, technical, or physical safeguards. *See Exhibit B, In re Twitter, Inc., C-4316, 151*
16 *F.T.C. 162 (Mar. 11, 2011) (Administrative Complaint) at ¶¶ 10-12.*

17 16. Twitter settled the Commission’s Administrative Complaint with the Commission Order.
18 The Commission Order became final in March 2011 and remains in effect.

19 17. Provision I of the Commission Order, in relevant part, states:

20 **IT IS ORDERED** that respondent, directly or through any corporation, subsidiary,
21 division, website, or other device, in connection with the offering of any product or service,
22 in or affecting commerce, shall not misrepresent in any manner, expressly or by
23 implication, the extent to which respondent maintains and protects the security, privacy,
24 confidentiality, or integrity of any nonpublic consumer information, including, but not
25 limited to, misrepresentations related to its security measures to: (a) prevent unauthorized
26 access to nonpublic consumer information; or (b) honor the privacy choices exercised by
27 users.

1 See Exhibit A, Commission Order, Provision I.

2 18. The Commission Order defines “nonpublic consumer information” as, in relevant part,
3 “an individual consumer’s: (a) email address... [and] (c) mobile telephone number[.]” See Exhibit A,
4 Commission Order, Definition 3.

5 **TWITTER’S NOTICE OF THE COMMISSION ORDER**

6 19. Twitter’s General Counsel signed the Commission Order on behalf of Twitter. The
7 Commission served the Commission Order in March 2011.

8 **NATURE OF THE CASE**

9 20. Twitter operates an online communication service through its website, www.twitter.com,
10 and through text messaging and mobile applications. The service allows registered users to
11 communicate with one another by posting “tweets,” or short messages currently limited to 280
12 characters or less, with which other users may interact through a “like,” reply, or “retweet.”

13 21. In order to follow other accounts, or post, like, and retweet tweets, users must register for
14 a Twitter account. The main page for a registered user who navigates to www.twitter.com or who opens
15 the Twitter mobile application, is known as a Twitter “timeline.” The timeline displays a stream of
16 tweets from accounts the user has chosen to follow. The timeline also displays a search engine,
17 recommendations for additional accounts to follow, and a list of trending topics. Registered users can
18 also navigate to their own profile page to view, among other things, their own tweets.

19 22. Twitter’s service is widely used. As of September 2019, Twitter had more than 330
20 million monthly active users worldwide, which includes journalists, celebrities, commercial brands, and
21 government officials.

22 23. Commercial entities regularly use Twitter to promote offers or advertise to consumers,
23 and many tweets contain links to other websites, including websites that users may use to purchase
24 commercial products or services.

25 24. Twitter’s core business model monetizes user information by using it for advertising. In
26 fact, of the \$3.4 billion in revenue that Twitter earned in 2019, \$2.99 billion flowed from advertising.

1 25. Twitter primarily allows companies to advertise on its service through “Promoted
2 Products,” which can take one of three forms: (1) Promoted Tweets, which appear within a user’s
3 timeline, search results, or profile pages, similar to an ordinary tweet; (2) Promoted Accounts, which
4 typically appear in the same format and place as other recommended accounts; and (3) Promoted
5 Trends, which appear at the top of the list of trending topics for an entire day.

6 26. Twitter offers various services that advertisers can use to reach their existing marketing
7 lists on Twitter, including “Tailored Audiences” and “Partner Audiences.” Tailored Audiences allows
8 advertisers to target specific groups of Twitter users by matching the telephone numbers and email
9 addresses that Twitter collects to the advertisers’ existing lists of telephone numbers and email
10 addresses. Partner Audiences allows advertisers to import marketing lists from data brokers like
11 Acxiom and Datalogix to match against the telephone numbers and email addresses collected by
12 Twitter. Twitter has provided advertisers the ability to match against lists of email addresses since
13 January 2014 and against lists of telephone numbers since September 2014.

14 27. Twitter has prompted users to provide a telephone number or email address for the
15 express purpose of securing or authenticating their Twitter accounts. However, through at least
16 September 2019, Twitter also used this information to serve targeted advertising and further its own
17 business interests through its Tailored Audiences and Partner Audiences services. For example, from at
18 least May 2013 until at least September 2019, Twitter collected telephone numbers and email addresses
19 from users specifically for purposes of allowing users to enable two-factor authentication, to assist with
20 account recovery (e.g., to provide access to accounts when users have forgotten their passwords), and to
21 re-authenticate users (e.g., to re-enable full access to an account after Twitter has detected suspicious or
22 malicious activity). From at least May 2013 through at least September 2019, Twitter did not disclose,
23 or did not disclose adequately, that it used these telephone numbers and email addresses to target
24 advertisements to those users through its Tailored Audiences and Partner Audiences services.

25 28. In 2011, after an FTC investigation, Twitter settled allegations that it had misrepresented
26 the extent to which Twitter protected the privacy and security of nonpublic consumer information. The
27 resulting Commission Order, among other things, prohibits Twitter from misrepresenting the extent to
28

1 which Twitter maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic
2 consumer information. *See* Exhibit A, Commission Order, Provision I.

3 29. More than 140 million Twitter users provided email addresses or telephone numbers to
4 Twitter based on Twitter’s deceptive statements that their information would be used for specific
5 purposes related to account security. Twitter knew or should have known that its conduct violated the
6 2011 Order, which prohibits misrepresentations concerning how Twitter maintains email addresses and
7 telephone numbers collected from users.

8 **TWITTER’S BUSINESS ACTIVITIES**

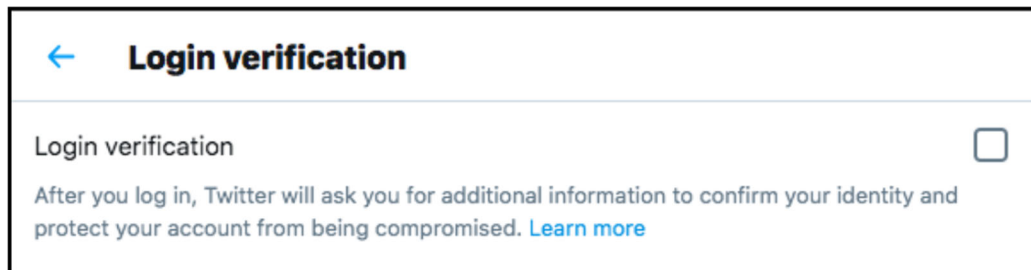
9 **Twitter Deceptively Used Information Provided for Two-Factor**

10 **Authentication to Serve Targeted Advertisements**

11 30. Since May 2013, Twitter has allowed users to log into Twitter with two-factor
12 authentication using their telephone numbers. Users who enable this security feature log into their
13 Twitter accounts with their usernames, passwords, and a code texted to their telephone numbers
14 whenever they log in from a new or unrecognized device.

15 31. Twitter prompts users to enable two-factor authentication through notices on their
16 timelines and after users reset their passwords. Twitter also encourages users to turn on two-factor
17 authentication in tweets from Twitter-operated accounts, Help Center documentation, and blog posts.

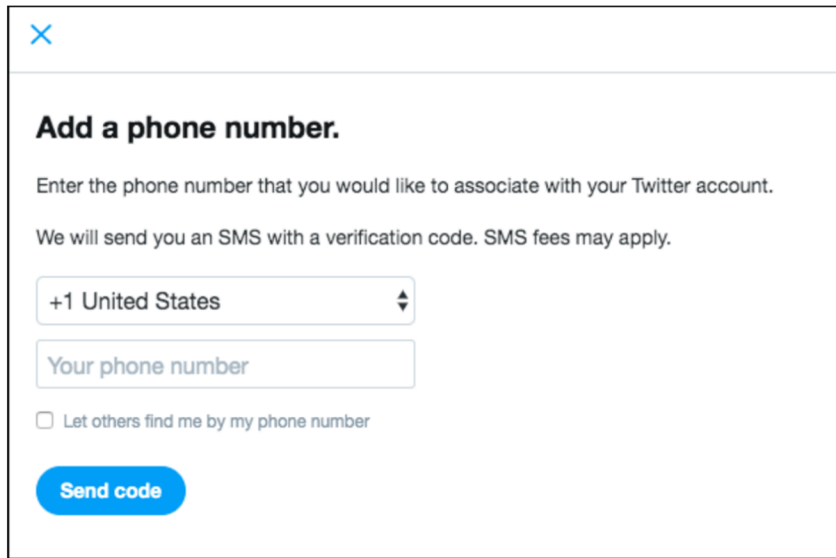
18 32. To enable two-factor authentication, Twitter users must navigate to an account settings
19 page. After clicking on “Security,” users see a screen similar to the one depicted below.



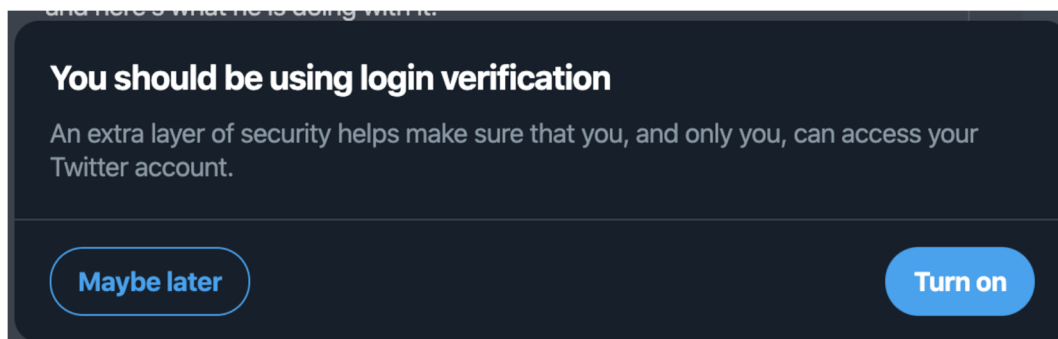
25 33. When users click on the “Learn more” link, they see a webpage that says, “How to use
26 two-factor authentication.” This page states, in relevant part:

1 Two-factor authentication is an extra layer of security for your Twitter account. Instead
2 of only entering a password to log in, you'll also enter a code or use a security key. This
3 additional step helps make sure that you, and only you, can access your account.

4 34. After clicking on the "Login Verification" checkbox above, users see additional
5 instructions about how to enable two-factor authentication. The last screen in the user flow related to
6 two-factor authentication using a telephone number is similar to the one depicted below:



7
8
9
10
11
12
13
14
15
16 35. Since at least September 2018, Twitter has prompted users to enable two-factor
17 authentication directly on users' timelines through a prompt similar to the screen depicted below:



18
19
20
21
22
23
24 36. Until September 2019, Twitter did not disclose at any point in the two-factor
25 authentication pathway or in any of the associated links described in Paragraphs 32 through 35 that it
26 was using the telephone numbers users provided for two-factor authentication to target advertisements to
27 those users.

1 37. From May 2013, approximately two million users provided a telephone number to enable
2 two-factor authentication.

3 38. The fact that Twitter used the telephone numbers provided for two-factor authentication
4 for advertising would be material to users when deciding whether to provide a telephone number for
5 two-factor authentication. In fact, public reaction to Twitter’s disclosure of this practice in late 2019
6 was largely negative, with one news outlet describing the practice as “particularly shameful.”

7 **Twitter Deceptively Used Information Provided for**
8 **Future Account Recovery to Serve Targeted Advertisements**

9 39. In June 2015, Twitter began prompting users to add a telephone number to their Twitter
10 accounts as a safeguard in the event of a lost password. Then, in April 2018, Twitter also began
11 prompting users to add an email address.

12 40. Since June 2015, if users do not have a telephone number associated with their accounts,
13 Twitter may prompt the users to add a telephone number through a message similar to the one depicted
14 below:



1 41. Similarly, since April 2018, if a user does not have an email address associated with their
2 account, Twitter may prompt the user to add an email address through a message similar to the one
3 depicted below:



4
5
6
7
8
9
10 42. Through September 2019, Twitter did not disclose at any point in the account recovery
11 pathway or any of the messages described in Paragraphs 40 and 41 that it was using the telephone
12 numbers or email addresses users provided for account recovery to target advertisements to those users.

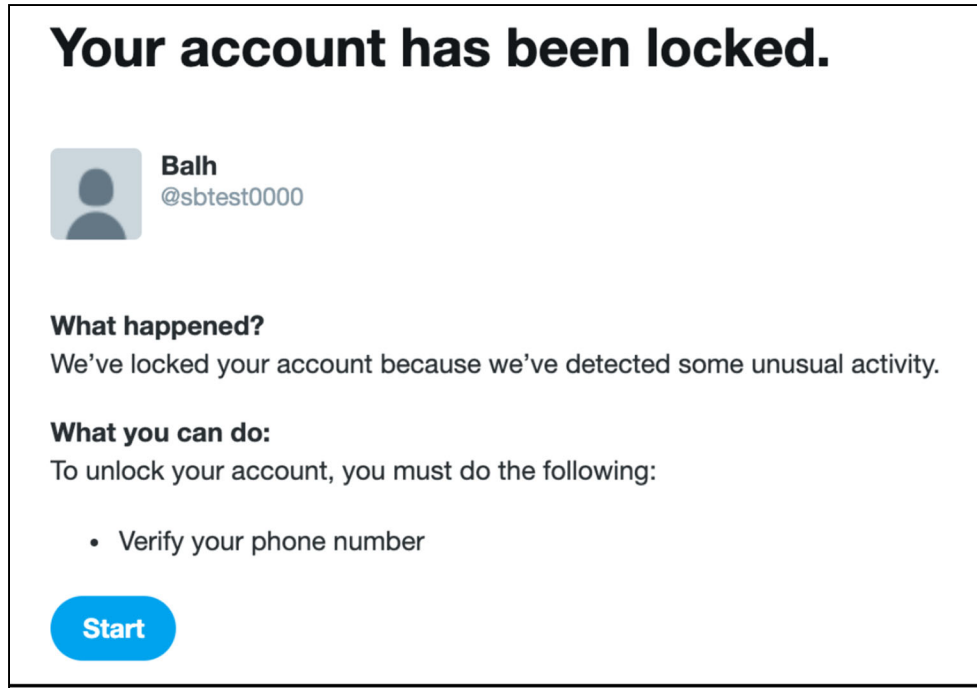
13 43. From June 2015, approximately 37 million users provided a telephone number or email
14 address for account recovery purposes.

15 44. The fact that Twitter used the telephone numbers and email addresses provided by users
16 to safeguard their accounts for advertising would be material to users when deciding whether to provide
17 their information for account recovery purposes.

18 **Twitter Deceptively Used Information Provided for**
19 **Re-authentication to Serve Targeted Advertisements**

20 45. In December 2013, Twitter began requiring users to provide a telephone number or email
21 address for re-authentication (e.g., to re-enable full access to an account after Twitter has detected
22 suspicious or malicious activity).

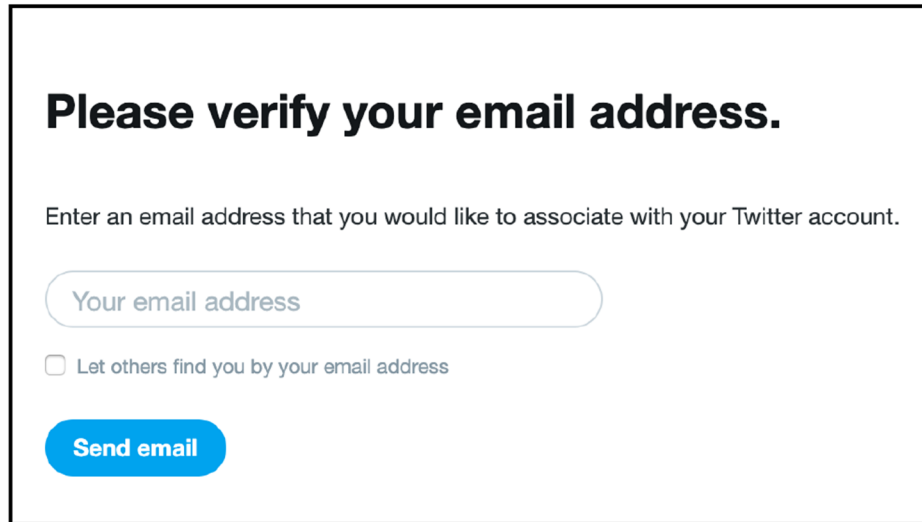
1 46. If Twitter detects suspicious or malicious activity on a user’s account, or suspects that the
2 account may belong to a previously-banned user, Twitter may require the user to re-authenticate by
3 providing a telephone number through a prompt similar to the one depicted below:



15 47. If users click the “Start” button pictured above, they are instructed to enter a telephone
16 number through a prompt similar to the one depicted below:



1 48. Similarly, Twitter may require users to provide an email address to re-enable full access
2 to their accounts with a prompt similar to the one depicted below:

A screenshot of a Twitter email verification prompt. The prompt is titled "Please verify your email address." in bold black text. Below the title, it says "Enter an email address that you would like to associate with your Twitter account." There is a text input field with the placeholder text "Your email address". Below the input field, there is a checkbox labeled "Let others find you by your email address". At the bottom of the prompt, there is a blue button with the text "Send email" in white.

3
4
5
6
7
8
9
10
11
12 49. Through September 2019, Twitter did not disclose at any point in the re-authentication
13 pathway described in Paragraphs 46 through 48 that it was using the telephone numbers or email
14 addresses users provided for re-authentication to target advertisements to those users.

15 50. From September 2014, approximately 104 million users provided a telephone number or
16 email address in response to a prompt for re-authentication.

17 51. The fact that Twitter used the telephone numbers and email addresses provided for
18 re-authentication for advertising would be material to users when deciding whether to provide their
19 information in response to a prompt for re-authentication.

20 **Twitter Misrepresented that it Processed Personal Data in Accordance with**
21 **the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks**

22 52. The European Union and Switzerland have each established regulatory regimes to protect
23 individuals' right to privacy with respect to the processing of their personal data. Both privacy regimes
24 generally prohibit businesses from transferring personal data to third countries unless the recipient
25 jurisdiction's laws are deemed to adequately protect personal data.

26 53. To ensure adequate privacy protections for commercial data transfers, the International
27 Trade Administration of the U.S. Department of Commerce ("Commerce") coordinated with the

1 European Commission and the Swiss Administration to craft the EU-U.S. and Swiss-U.S. Privacy Shield
2 Frameworks (“Privacy Shield” or “Frameworks”). The Frameworks are materially identical.

3 54. To rely on the Privacy Shield for data transfers, a company needed to self-certify and
4 annually affirm to Commerce that it complied with the Privacy Shield Principles (the “Principles”). Of
5 note, Principle 5(a) provided that “[a]n organization may not process personal information in a way that
6 is incompatible with the purposes for which it has been collected or subsequently authorized by the
7 individual.” The Frameworks defined “processing” to include “any operation or set of operations which
8 is performed upon personal data, whether or not by automated means” and includes, among other things,
9 “collection,” “storage,” and “use” of personal information.

10 55. Companies under the enforcement jurisdiction of the FTC, as well as the U.S.
11 Department of Transportation, were eligible to join the EU-U.S. and Swiss-U.S. Privacy Shield
12 Frameworks. A company under the FTC’s jurisdiction that self-certified to the Privacy Shield
13 Principles, but failed to comply with the Privacy Shield, may be subject to an enforcement action based
14 on the FTC’s deception authority under Section 5 of the FTC Act.

15 56. Commerce maintains a public website, <https://www.privacyshield.gov>, where it posts the
16 names of companies that have self-certified to the Privacy Shield. The listing of companies, found at
17 <https://www.privacyshield.gov/list>, indicates whether the company’s self-certification is current.

18 57. On November 16, 2016, Twitter self-certified its participation in the Privacy Shield.
19 Twitter has reaffirmed its participation in the Privacy Shield to Commerce each year thereafter.

20 58. As described in Paragraphs 30 through 51, through at least September 2019, Twitter
21 deceptively used personal information collected for specific security-related purposes for advertising.
22 Twitter’s use of such personal information for advertising purposes was not compatible with the
23 purposes for which the information was collected, and Twitter did not obtain subsequent authorization
24 from any individual to use such information for advertising.

25 **Ongoing Conduct**

26 59. Based on the facts and violations of law alleged in this Complaint, the FTC has reason to
27 believe that Twitter is violating or is about to violate laws enforced by the Commission. Among other
28

1 things, Twitter is a recidivist that engaged in unlawful conduct even after law enforcement action. In
2 addition, Twitter still makes most of its money by directing advertisements to its users, including by
3 targeting particular users based on information the users provide. Therefore, Twitter has an incentive to
4 resume its unlawful conduct, and it retains the means and ability to do so. Twitter also engaged in the
5 unlawful conduct at issue here from at least January 2014 through at least September 2019—a period of
6 almost six years.

7 **VIOLATIONS OF THE FTC ACT**

8 **Count 1—Deceptive Practices Regarding the Use of Telephone**

9 **Numbers Provided for Two-Factor Authentication**

10 60. Paragraphs 1 through 59 are incorporated as if set forth herein.

11 61. As described above in Paragraphs 30 through 38, Twitter represented, directly or
12 indirectly, expressly or by implication, that users’ telephone numbers provided for two-factor
13 authentication would be used for security purposes.

14 62. In numerous instances in which Twitter has made the representation set forth in
15 Paragraph 61, Twitter failed to disclose, or failed to disclose adequately, that Twitter would also use
16 telephone numbers provided by users for two-factor authentication for targeting advertisements to those
17 users.

18 63. Twitter’s failure to disclose or disclose adequately the material information described in
19 Paragraph 62, in light of the representations set forth in Paragraph 61, is a deceptive act or practice in
20 violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

21 **Count 2—Deceptive Practices Regarding the Use of Telephone Numbers**
22 **and Email Addresses Provided for Account Recovery**

23 64. Paragraphs 1 through 59 are incorporated as if set forth herein.

24 65. As described above in Paragraphs 39 through 44, Twitter represented, directly or
25 indirectly, expressly or by implication, that users’ telephone numbers and email addresses provided for
26 account recovery would be used for security purposes.

1 66. In numerous instances in which Twitter has made the representation set forth in
2 Paragraph 65, Twitter failed to disclose, or failed to disclose adequately, that Twitter would also use
3 telephone numbers and email addresses provided by users for account recovery for targeting
4 advertisements to those users.

5 67. Twitter’s failure to disclose or disclose adequately the material information described in
6 Paragraph 66, in light of the representations set forth in Paragraph 65, is a deceptive act or practice in
7 violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

8 **Count 3—Deceptive Practices Regarding the Use of Telephone Numbers**
9 **and Email Addresses Provided for Re-authentication**

10 68. Paragraphs 1 through 59 are incorporated as if set forth herein.

11 69. As described above in Paragraphs 45 through 51, Twitter represented, directly or
12 indirectly, expressly or by implication, that users’ telephone numbers and email addresses provided for
13 account re-authentication would be used for security purposes.

14 70. In numerous instances in which Twitter has made the representation set forth in
15 Paragraph 69, Twitter failed to disclose, or failed to disclose adequately, that Twitter would also use
16 telephone numbers and email addresses provided by users for account re-authentication for targeting
17 advertisements to those users.

18 71. Twitter’s failure to disclose or disclose adequately the material information described in
19 Paragraph 70, in light of the representations set forth in Paragraph 69, is a deceptive act or practice in
20 violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

21 **Count 4—Deceptive Practices Regarding Twitter’s Compliance**
22 **with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks**

23 72. Paragraphs 1 through 59 are incorporated as if set forth herein.

24 73. As described in Paragraph 57, Twitter has represented, directly or indirectly, expressly or
25 by implication, that it has complied with the Privacy Shield Principles since at least November 16, 2016.

26 74. In fact, as described in Paragraph 58, until at least September 2019, Twitter failed to
27 comply with the Privacy Shield Principles’ requirement that it may not process personal information in a
28

1 way that is incompatible with the purposes for which it was collected or subsequently authorized by the
2 individual about whom the information pertains. Therefore, the representation set forth in Paragraph 73
3 was false or misleading.

4 75. The acts and practices of Twitter as alleged in this Complaint constitute unfair or
5 deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade
6 Commission Act, 15 U.S.C. § 45(a).

7 **VIOLATIONS OF THE COMMISSION ORDER**

8 76. Each representation Twitter has made in violation of the Commission Order constitutes a
9 separate violation for which Plaintiff may seek a civil penalty pursuant to Section 5(l) of the FTC Act,
10 15 U.S.C. § 45(l).

11 77. Section 5(l) of the FTC Act, 15 U.S.C. § 45(l), as modified by Section 4 of the Federal
12 Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461, and Section 1.98(c) of the FTC’s
13 Rules of Practice, 16 C.F.R. § 1.98(c), directs that a defendant who violates an order of the Commission
14 after it has become final, and while such order is in effect, “shall forfeit and pay to the United States a
15 civil penalty of not more than \$46,517 for each violation.”

16 78. Sections 5(l) and 13(b) of the FTC Act, 15 U.S.C. §§ 45(l) and 53(b), also authorize this
17 Court to grant an “injunction[] and such other and further equitable relief” as it may deem appropriate to
18 halt and redress violations of any provision of law enforced by the FTC Act and to enforce the
19 Commission Order.

20 **Count 5—Misrepresenting the Extent to Which Twitter Maintains and**
21 **Protects the Privacy of Nonpublic Consumer Information as it Relates**
22 **to Telephone Numbers Provided for Two-Factor Authentication**

23 79. Paragraphs 1 through 59 are incorporated as if set forth herein.

24 80. Provision I of the Commission Order prohibits Twitter from misrepresenting “the extent
25 to which [Twitter] maintains and protects the security, privacy, confidentiality, or integrity of any
26 nonpublic consumer information, including, but not limited to, misrepresentations related to its security
27
28

1 measures to: (a) prevent unauthorized access to nonpublic consumer information; or (b) honor the
2 privacy choices exercised by users.”

3 81. As described above in Paragraphs 30 through 38, Twitter represented, directly or
4 indirectly, expressly or by implication, that it would maintain and protect the privacy of users’ telephone
5 numbers collected specifically for purposes of enabling two-factor authentication.

6 82. In fact, Twitter failed to disclose, or failed to disclose adequately, that Twitter would also
7 use the telephone numbers described in Paragraph 81 for targeted advertising.

8 83. Twitter’s failure to disclose or disclose adequately the material information described in
9 Paragraph 82, in light of the representations set forth in Paragraph 81, misrepresented the extent to
10 which Twitter maintains and protects the privacy of nonpublic consumer information.

11 84. Therefore, the representations described in Paragraph 81 violated Provision I of the
12 Commission Order.

13 **Count 6—Misrepresenting the Extent to Which Twitter Maintains and Protects**
14 **the Privacy of Nonpublic Consumer Information as it Relates to Telephone**
15 **Numbers and Email Addresses Provided for Account Recovery**

16 85. Paragraphs 1 through 59 are incorporated as if set forth herein.

17 86. Provision I of the Commission Order prohibits Twitter from misrepresenting “the extent
18 to which [Twitter] maintains and protects the security, privacy, confidentiality, or integrity of any
19 nonpublic consumer information, including, but not limited to, misrepresentations related to its security
20 measures to: (a) prevent unauthorized access to nonpublic consumer information; or (b) honor the
21 privacy choices exercised by users.”

22 87. As described above in Paragraphs 39 through 44, Twitter represented, directly or
23 indirectly, expressly or by implication, that it would maintain and protect the privacy of users’ telephone
24 numbers and email addresses collected for purposes of account recovery.

25 88. In fact, Twitter failed to disclose, or failed to disclose adequately, that Twitter would also
26 use the telephone numbers and email addresses described in Paragraph 87 for targeted advertising.

1 89. Twitter’s failure to disclose or disclose adequately the material information described in
2 Paragraph 88, in light of the representations set forth in Paragraph 87, misrepresented the extent to
3 which Twitter maintains and protects the privacy of nonpublic consumer information.

4 90. Therefore, the representations described in Paragraph 87 violated Provision I of the
5 Commission Order.

6 **Count 7—Misrepresenting the Extent to Which Twitter Maintains and Protects**
7 **the Privacy of Nonpublic Consumer Information as it Relates to Telephone**
8 **Numbers and Email Addresses Provided for Re-authentication**

9 91. Paragraphs 1 through 59 are incorporated as if set forth herein.

10 92. Provision I of the Commission Order prohibits Twitter from misrepresenting “the extent
11 to which [Twitter] maintains and protects the security, privacy, confidentiality, or integrity of any
12 nonpublic consumer information, including, but not limited to, misrepresentations related to its security
13 measures to: (a) prevent unauthorized access to nonpublic consumer information; or (b) honor the
14 privacy choices exercised by users.”

15 93. As described above in Paragraphs 45 through 51, Twitter represented, directly or
16 indirectly, expressly or by implication, that it would maintain and protect the privacy of users’ telephone
17 numbers and email addresses collected to re-authenticate a user’s Twitter account.

18 94. In fact, Twitter failed to disclose, or failed to disclose adequately, that Twitter would also
19 use the telephone numbers and email addresses described in Paragraph 93 for targeted advertising.

20 95. Twitter’s failure to disclose or disclose adequately the material information described in
21 Paragraph 94, in light of the representations set forth in Paragraph 93, misrepresented the extent to
22 which Twitter maintains and protects the privacy of nonpublic consumer information.

23 96. Therefore, the representations described in Paragraph 93 violated Provision I of the
24 Commission Order.

25 **CONSUMER INJURY**

26 97. Consumers have suffered and will continue to suffer substantial injury as a result of
27 Twitter’s violations of the FTC Act and the 2011 Order. In addition, Twitter has been unjustly enriched

1 as a result of its unlawful acts or practices. Absent injunctive relief by this Court, Twitter is likely to
2 continue to injure consumers, reap unjust enrichment, and harm the public interest.

3 **PRAYER FOR RELIEF**

4 98. WHEREFORE, Plaintiff requests that the Court:

- 5 A. Enter judgment against Twitter and in favor of Plaintiff for violating the 2011
6 Order and the FTC Act as alleged in this Complaint;
- 7 B. Award Plaintiff monetary civil penalties from Twitter for each violation of the
8 2011 Order;
- 9 C. Enter a permanent injunction to prevent future violations by Twitter of the 2011
10 Order, or as it is subsequently modified by operation of law, and the FTC Act;
- 11 D. Award monetary and other relief within the Court's power to grant; and
- 12 E. Award any additional relief as the Court determines to be just and proper.
- 13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 Dated: May 25, 2022

Respectfully submitted,

2 FOR THE UNITED STATES OF AMERICA:

3 *Of Counsel:*

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division

4 JAMES A. KOHM
5 Associate Director
6 Division of Enforcement

ARUN G. RAO
Deputy Assistant Attorney General

7 LAURA KOSS
8 Assistant Director
9 Division of Enforcement

GUSTAV W. EYLER
Director
Consumer Protection Branch

9 REENAH L. KIM
10 Attorney
11 Division of Enforcement

LISA K. HSIAO
Assistant Director

11 ANDREA V. ARIAS
12 Attorney
13 Division of Privacy and Identity Protection

/s/ Zachary L. Cowan
ZACHARY L. COWAN
DEBORAH S. SOHN
Trial Attorneys
Consumer Protection Branch
U.S. Department of Justice
450 5th Street, N.W. Suite 6400-S
Washington, D.C. 20530
Tel: (202) 598-7566
Fax: (202) 514-8742
Zachary.L.Cowan@usdoj.gov
Deborah.S.Sohn@usdoj.gov

14 Federal Trade Commission
15 600 Pennsylvania Avenue, N.W.,
16 Mail Stop CC-9528
17 Washington, D.C. 20580
18 Tel: (202) 326-2272 (Kim)
Tel: (202) 326-2715 (Arias)
rkim1@ftc.gov
aarias@ftc.gov

19 STEPHANIE M. HINDS
20 United States Attorney

21 MICHELLE LO
22 Chief
23 Civil Division

24 SHARANYA MOHAN
25 EMMET P. ONG
26 Assistant United States Attorneys
27 Northern District of California
28 450 Golden Gate Avenue
San Francisco, CA 94102
Tel: (415) 436-7198
sharanya.mohan@usdoj.gov
emmet.ong@usdoj.gov

EXHIBIT A

092 3093

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS: Jon Leibowitz, Chairman
William E. Kovacic
J. Thomas Rosch
Edith Ramirez
Julie Brill**

In the Matter of

TWITTER, INC.,
a corporation.

DOCKET NO: C-4316

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq.*;

The respondent and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by the respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments received from interested persons, now in further conformity with the procedure described in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its Complaint, makes the following jurisdictional findings, and enters the following Order:

1. Respondent Twitter, Inc. (“Twitter”) is a Delaware corporation with its principal office or place of business at 795 Folsom Street, Suite 600, San Francisco, CA 94103.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean Twitter, its successors and assigns, officers, agents, representatives, and employees.
2. “Consumer” shall mean any person, including, but not limited to, any user of respondent’s services, any employee of respondent, or any individual seeking to become an employee, where “employee” shall mean an agent, servant, salesperson, associate, independent contractor, or other person directly or indirectly under the control of respondent.
3. “Nonpublic consumer information” shall mean nonpublic, individually-identifiable information from or about an individual consumer, including, but not limited to, an individual consumer’s: (a) email address; (b) Internet Protocol (“IP”) address or other persistent identifier; (c) mobile telephone number; and (d) nonpublic communications made using respondent’s microblogging platform. “Nonpublic consumer information” shall not include public communications made using respondent’s microblogging platform.
4. “Administrative control of Twitter” shall mean the ability to access, modify, or operate any function of the Twitter system by using systems, features, or credentials that were designed exclusively for use by authorized employees or agents of Twitter.
5. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, website, or other device, in connection with the offering of any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which respondent maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information, including, but not limited to, misrepresentations related to its security measures to: (a) prevent unauthorized access to nonpublic consumer information; or (b) honor the privacy choices exercised by users.

II.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, website, or other device, in connection with the offering of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the nonpublic consumer information, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program.
- B. the identification of reasonably-foreseeable, material risks, both internal and external, that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of nonpublic consumer information or in unauthorized administrative control of the Twitter system, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, account takeovers, or other systems failures.
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding nonpublic consumer information such service providers receive from respondent or obtain on respondent's behalf, and the requirement, by contract, that such service providers implement and maintain appropriate safeguards; provided, however, that this subparagraph shall not apply to personal information about a consumer that respondent provides to a government agency or lawful information supplier when the agency or supplier already possesses the information and uses it only to retrieve, and supply to respondent, additional personal information about the consumer.

E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Paragraph II of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for ten (10) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the nonpublic personal information collected from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by Paragraph II of this order; and
- D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information and that the program has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

IV.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

- A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely-disseminated statements, including, but not limited to, statements posted on respondent's website that describe the extent to which respondent maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information, with all materials relied upon in making or disseminating such statements, except that respondent shall not be required to provide any such statements that are made using the Twitter microblogging platform;
- B. for a period of six (6) months from the date received, all consumer complaints directed at respondent, or forwarded to respondent by a third party, that relate to respondent's activities as alleged in the draft complaint and any responses to such complaints;
- C. for a period of two (2) years from the date received, copies of all subpoenas and other communications with law enforcement entities or personnel, if such communications raise issues that relate to respondent's compliance with the provisions of this order;
- D. for a period of five (5) years from the date received, any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- E. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

V.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VII.

IT IS FURTHER ORDERED that respondent shall, within sixty (60) days after the date of service of this order file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form in which respondent has complied with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, respondent shall submit additional true and accurate written reports.

VIII.

This order will terminate on March 2, 2031, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

- A. any Part in this order that terminates in fewer than twenty (20) years;
- B. this order if such complaint is filed after the order has terminated pursuant to this Part.

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 as to such respondent will terminate according to this Part 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.

Donald S. Clark
Secretary

SEAL

ISSUED: March 2, 2011

EXHIBIT B

092-3093

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of

TWITTER, INC.,
a corporation.

DOCKET NO. C-4316

COMPLAINT

The Federal Trade Commission, having reason to believe that Twitter, Inc. (“Twitter” or “respondent”), a corporation, has violated the Federal Trade Commission Act (“FTC Act”), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Twitter is a privately-owned, Delaware corporation with its principal office or place of business at 795 Folsom St., Suite 600, San Francisco, CA 94103.
2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act.

RESPONDENT’S BUSINESS PRACTICES

3. Since approximately July 2006, Twitter has operated www.twitter.com, a social networking website that enables users to send “tweets” – brief updates of 140 characters or less – to their “followers” (*i.e.*, users who sign up to receive such updates) via email and phone text. Consumers who use Twitter can follow other individuals, as well as commercial, media, governmental, or nonprofit entities. Using Twitter, consumers may receive discount offers from companies, breaking news from media outlets, and public safety and emergency updates from federal and municipal authorities. In many instances, tweets invite users to click on links to other websites, including websites that consumers may use to obtain commercial products or services.
4. Twitter collects certain information from each user and makes it part of the user’s public profile. Such information includes: a user name and profile image, lists of the other Twitter users whom the user follows and is followed by, and, at the user’s option, a website address, location, time zone, and one-line narrative description or “bio.” In addition, tweets appear in the user profile for both sender and recipient – and are public – except where users “protect” their tweets or send “direct messages,” as described in **paragraph 6**, below.
5. Twitter also collects certain information about its users that it does not make public. Such information includes: an email address, Internet Protocol (“IP”) addresses, mobile

carrier or mobile telephone number (for users who receive updates by phone), and the username for any Twitter account that a user has chosen to “block” from exchanging tweets with the user. This nonpublic information (collectively, “nonpublic user information”) cannot be viewed by other users or any other third parties, but – with the exception of IP addresses – can be viewed by the user who operates the account.

6. Twitter offers privacy settings through which a user may choose to designate tweets as nonpublic. For example, Twitter offers users the ability to send “direct messages” to a specified follower and states that “only author and recipient can view” such messages. Twitter also allows users to click a button labeled “Protect my tweets.” If a user chooses this option, Twitter states that the user’s tweets can be viewed only by the user’s approved followers. Unless deleted, direct messages and protected tweets (collectively, “nonpublic tweets”) are stored in the recipient’s Twitter account.
7. From approximately July 2006 until July 2009, Twitter granted almost all of its employees the ability to exercise administrative control of the Twitter system, including the ability to: reset a user’s account password, view a user’s nonpublic tweets and other nonpublic user information, and send tweets on behalf of a user. Such employees have accessed these administrative controls using administrative credentials, composed of a user name and administrative password.
8. From approximately July 2006 until January 2009, Twitter’s employees entered their administrative credentials into the same webpage where users logged into www.twitter.com (hereinafter, “public login webpage”).
9. From approximately July 2006 until July 2008, Twitter did not provide a company email account. Instead, it instructed each employee to use a personal email account of the employee’s choice for company business. During this time, company-related emails from Twitter employees in many instances displayed the employee’s personal email address in the email header.

RESPONDENT’S STATEMENTS

10. Respondent has disseminated or caused to be disseminated statements to consumers on its website regarding its operation and control of the Twitter system, including, but not limited to:
 - a. from approximately May 2007 until November 2009, the following statement in Twitter’s privacy policy regarding Twitter’s protection of nonpublic user information:

Twitter is very concerned about safeguarding the confidentiality of your personally identifiable information. We employ administrative, physical, and electronic measures designed to protect your information from unauthorized access. (*See Exhibit 1*).

- b. since approximately November 17, 2008, the following statements on its website regarding the privacy of direct messages that users send via Twitter:

**Help Resources/Getting Started/What is a direct message?
What is a direct message? (DM)**

Private Twitter Messages

In addition to public updates . . . you can send followers private tweets, called direct messages, too . . .

[direct messages] are not public; only author and recipient can view direct messages. (*See Exhibit 2; emphases in original*).

- c. since at least November 6, 2008, the following statements on its website regarding the privacy of protected tweets that users send via Twitter:

Public vs protected accounts

. . .

Public or protected (private)?

When you sign up for Twitter, you have the option of keeping your account public (the default account setting) or protecting the account to keep your updates private . . . Protected accounts receive a follow request each time someone wants to follow them, and only approved followers are able to see the profile page. If the idea of strangers reading your Twitter updates makes you feel a little weird, try protecting your profile at first. You can always change your mind later. . . .

Protecting your Twitter profile

Not everyone has to see your Twitter updates. Keep your Twitter updates private and approve your followers by protecting your profile . . . Protected account owners control who is able to follow them, and keep their updates away from the public eye . . . (*See Exhibit 3; emphases in original*).

RESPONDENT'S SECURITY PRACTICES

11. Contrary to the statements above, Twitter has engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security to: prevent unauthorized access to nonpublic user information and honor the privacy choices exercised by its users in designating certain tweets as nonpublic. In particular, Twitter failed to prevent unauthorized administrative control of the Twitter system by, among other things, failing to:

- a. establish or enforce policies sufficient to make administrative passwords hard to guess, including policies that: (1) prohibit the use of common dictionary words as administrative passwords; and (2) require that such passwords be unique – *i.e.*, different from any password that the employee uses to access third-party programs, websites, and networks;
 - b. establish or enforce policies sufficient to prohibit storage of administrative passwords in plain text in personal email accounts;
 - c. suspend or disable administrative passwords after a reasonable number of unsuccessful login attempts;
 - d. provide an administrative login webpage that is made known only to authorized persons and is separate from the login webpage provided to other users;
 - e. enforce periodic changes of administrative passwords, such as by setting these passwords to expire every 90 days;
 - f. restrict each person's access to administrative controls according to the needs of that person's job; and
 - g. impose other reasonable restrictions on administrative access, such as by restricting access to specified IP addresses.
12. Between January and May 2009, intruders exploited the failures described above in order to obtain unauthorized administrative control of the Twitter system. Through this administrative control, the intruders were able to: (1) gain unauthorized access to nonpublic tweets and nonpublic user information, and (2) reset any user's password and send unauthorized tweets from any user account. In particular:
- a. On approximately January 4, 2009, an intruder used an automated password guessing tool to derive an employee's administrative password, after submitting thousands of guesses into Twitter's public login webpage. The password was a weak, lowercase, letter-only, common dictionary word. Using this password, the intruder could access nonpublic user information and nonpublic tweets for any Twitter user. In addition, the intruder could, and did, reset user passwords, some of which the intruder posted on a website. Thereafter, certain of these fraudulently-reset user passwords were obtained and used by other intruders to send unauthorized tweets from user accounts, including one tweet, purportedly from Barack Obama, that offered his more than 150,000 followers a chance to win \$500 in free gasoline, in exchange for filling out a survey. Unauthorized tweets also were sent from eight (8) other accounts, including the Fox News account.

- b. On approximately April 27, 2009, an intruder compromised an employee's personal email account, and was able to infer the employee's Twitter administrative password, based on two similar passwords, which had been stored in the account, in plain text, for at least six (6) months prior to the attack. Using this password, the intruder could access nonpublic user information and nonpublic tweets for any Twitter user. In addition, the intruder could, and did, reset at least one user's password.

VIOLATIONS OF THE FTC ACT

Count 1

13. As set forth in **paragraph 10**, respondent has represented, expressly or by implication, that it uses reasonable and appropriate security measures to prevent unauthorized access to nonpublic user information.
14. In truth and in fact, as described in **paragraph 11**, respondent did not use reasonable and appropriate security measures to prevent unauthorized access to nonpublic user information. Therefore, the representation set forth in **paragraph 13** was, and is, false or misleading.

Count 2

15. As set forth in **paragraph 10**, respondent has represented, expressly or by implication, that it uses reasonable and appropriate security measures to honor the privacy choices exercised by users.
16. In truth and in fact, as described in **paragraph 11**, respondent did not use reasonable and appropriate security measures to honor the privacy choices exercised by users. Therefore, the representation set forth in **paragraph 15** was, and is, false or misleading.
17. The acts and practices of respondent as alleged in this complaint constitute deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this second day of March, 2011, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

EXHIBIT 1

- [Skip past navigation](#)
- On a mobile phone? Check out m.twitter.com!
- [Skip to navigation](#)
- [Skip to sign in form](#)



- [Login](#)
- [Join Twitter!](#)

Twitter Privacy Policy

This Privacy Policy is effective as of May 14, 2007.

Twitter provides this Privacy Policy to inform users of our policies and procedures regarding the collection, use and disclosure of personally identifiable information received from users of this website, located at www.twitter.com ("Site") or collected through our social networking service, including via SMS, WAP and Instant Messaging ("Service"). This Privacy Policy may be updated from time to time for any reason; each version will apply to information collected while it was in place. We will notify you of any material changes to our Privacy Policy by posting the new Privacy Policy on our Site. You are advised to consult this Privacy Policy regularly for any changes.

By using our Site you are consenting to our processing of your information as set forth in this Privacy Policy now and as amended by us. "Processing" means using cookies on a computer or using or touching information in any way, including, but not limited to, collecting, storing, deleting, using, combining and disclosing information, all of which activities will take place in the United States. If you reside outside the U.S. your personally identifiable information will be transferred to the U.S., and processed and stored there under U.S. privacy standards. By visiting our Site and providing information to us, you consent to such transfer to, and processing in, the US.

If you have any questions or comments about this Privacy Policy or our use of your personally identifiable information, please contact us at [privacy at twitter dot com](mailto:privacy@twitter.com).

Information Collection and Use

Our primary goals in collecting personally identifiable information are to provide you with the product and services made available through the Site, including, but not limited, to the Service, to communicate with you, and to manage your registered user account, if you have one.

Information Collected Upon Registration. If you desire to have access to certain restricted sections of the Site, you will be required to become a registered user, and to submit certain personally identifiable information to Twitter. This happens in a number of instances, such as when you sign up for the Service, or if you desire to receive marketing materials and information. Personally identifiable information that we may collect in such instances may include your IP address, full user name, password, email address, city, time zone, telephone number, and other information that you decide to provide us with, or that you decide to include in your public profile.

Additional Information Your full user name and your photo, if you decide to upload one, are displayed to people in the Twitter network to enable you to connect with people on Twitter, as specified in your privacy settings. Once a member, you may provide additional information in the profile section, including but not limited to your bio, your location, as well as your personal web site, if you have one. Providing additional information beyond what is required at registration is entirely optional, but enables you to better identify yourself and find new friends and opportunities in the Twitter system. If you activate the mobile phone options per the Terms of Service at www.twitter.com/tos, we will collect your cellular phone number account information. You will receive notifications on your cellular phone account in a number of cases, such as when a Twitter member adds you as a friend or sends you a message. If you contact us by email through the Site, we may keep a record of your contact information and correspondence, and may use your email address, and any information that you provide to us in your message, to respond to you.

Use of Contact Information In addition, we may use your contact information to market to you, and provide you with information about, our products and services, including but not limited to our Service. If you decide at any time that you no longer wish to receive such information or communications from us, please follow the unsubscribe instructions provided in any of the communications.

Log Data When you visit the Site, our servers automatically record information that your browser sends whenever you visit a website ("Log Data"). This Log Data may include information such as your IP address, browser type or the domain from which you are visiting, the web-pages you visit, the search terms you use, and any advertisements on which you click. For most users accessing the Internet from an Internet service provider the IP address will be different every time you log on. We use Log Data to monitor the use of the Site and of our Service, and for the SiteTMs technical administration. We do not associate your IP address with any other personally identifiable information to identify you personally, except in case of violation of the Terms of Service

Cookies

Like many websites, we also use "cookie" technology to collect additional website usage data and to improve the Site and our service. A cookie is a small data file that we transfer to your computerTMs hard disk. We do not use cookies to collect personally identifiable information. Twitter may use both session cookies and persistent cookies to better understand how you interact with the Site and our Service, to monitor aggregate usage by our users and web traffic routing on the Site, and to improve the Site and our services. A session cookie enables certain features of the Site and our service and is deleted from your computer when you disconnect from or leave the Site. A persistent cookie remains after you close your browser and may be used by your browser on subsequent visits to the Site. Persistent cookies can be removed by following your web browser help file directions. Most Internet browsers automatically accept cookies. You can instruct your browser, by editing its options, to stop accepting cookies or to prompt you before accepting a cookie from the websites you visit.

Information Sharing and Disclosure

Service Providers We engage certain trusted third parties to perform functions and provide services to us, including, without limitation, hosting and maintenance, customer relationship, database storage and management, and direct marketing campaigns. We will share your personally identifiable information with these third parties, but only to the extent necessary to perform these functions and provide such services, and only pursuant to binding contractual obligations requiring

such third parties to maintain the privacy and security of your data.

Compliance with Laws and Law Enforcement Twitter cooperates with government and law enforcement officials or private parties to enforce and comply with the law. We may disclose any information about you to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate to respond to claims, legal process (including subpoenas), to protect the property and rights of Twitter or a third party, the safety of the public or any person, to prevent or stop any illegal, unethical, or legally actionable activity, or to comply with the law.

Business Transfers Twitter may sell, transfer or otherwise share some or all of its assets, including your personally identifiable information, in connection with a merger, acquisition, reorganization or sale of assets or in the event of bankruptcy. You will have the opportunity to opt out of any such transfer if the new entity's planned processing of your information differs materially from that set forth in this Privacy Policy.

Changing or Deleting Information

If you are a registered user of the Site, you may access and update or correct the information you provided to us by e-mailing us at [privacy at twitter dot com](mailto:privacy@twitter.com).

Security

Twitter is very concerned about safeguarding the confidentiality of your personally identifiable information. We employ administrative, physical and electronic measures designed to protect your information from unauthorized access.

We will make any legally-required disclosures of any breach of the security, confidentiality, or integrity of your unencrypted electronically stored personal data to you via email or conspicuous posting on this Site in the most expedient time possible and without unreasonable delay, consistent with (i) the legitimate needs of law enforcement or (ii) any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Links to Other Websites

Our Site contains links to other websites. The fact that we link to a website is not an endorsement, authorization or representation of our affiliation with that third party. We do not exercise control over third party websites. These other websites may place their own cookies or other files on your computer, collect data or solicit personally identifiable information from you. Other sites follow different rules regarding the use or disclosure of the personally identifiable information you submit to them. We encourage you to read the privacy policies or statements of the other websites you visit.

Our Policy Towards Children

The Site is not directed to persons under 13. If a parent or guardian becomes aware that his or her child has provided us with personally identifiable information without their consent, he or she should contact us at [privacy at twitter dot com](mailto:privacy@twitter.com). We do not knowingly collect personally identifiable information from children under 13. If we become aware that a child under 13 has provided us with personal identifiable Information, we will delete such information from our files.

Footer

- [© 2009 Twitter](#)
 - [About Us](#)
 - [Contact](#)
 - [Blog](#)
 - [Status](#)
 - [Goodies](#)
 - [API](#)
 - [Business](#)
 - [Help](#)
 - [Jobs](#)
 - [Terms](#)
 - [Privacy](#)
-

EXHIBIT 2

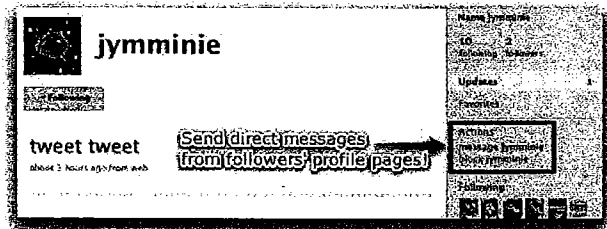
Help Resources / Getting Started / What is a direct message?...

What is a direct message? (DM)

Submitted Nov 17, 2008 by crystal

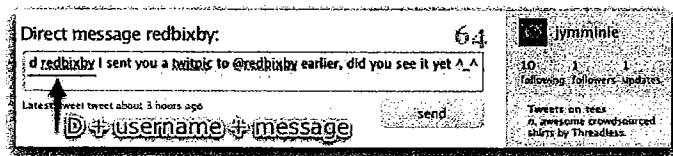
Private Twitter Messages

In addition to public updates and @replies, you can send followers private tweets, called direct messages, too. If someone is following you, you can send a direct message from the web via the "message" link on the profile page. (please note: you cannot send a direct message to a user who is not following you.)



You can also send direct messages from:

- the reply icon attached to messages in your direct message inbox
- the drop down box on the direct message inbox page (please note: this is a random selection of people who are following you, not the complete list. If a follower's name is not on this list, use the options above or below)
- the status update box using the direct message command: d + username + message



Tip: to reply to a regular Twitter update with a direct message from your home page, click the arrow/swoosh at the end of an update; this sets an @reply in the update box. Remove the @ sign and replace it with a "d" and a space, and type the message. People who have their direct message text and email notifications set to ON will receive direct messages on their phones and/or via email. Tweets sent using any of the methods described above are not public: only author and recipient can view direct messages.

More like tweets, less like email

Direct messages behave more like tweets than emails: any action the sender of a DM takes on a direct message will affect the recipient of that DM. As the recipient of the Direct Message, you have the ability to delete it; the messages you delete also disappear from the sender's sent tab. Conversely, deleting direct messages you have sent will also delete the message from the recipient's inbox forever.

The number next to your Direct Messages tab reflects the number of direct messages in your inbox. If this number has changed recently and you have not deleted any of your messages, remember: the sender of the direct message has the ability to delete messages from your inbox, these messages are not mysteriously disappearing or getting lost.

Direct messaging from your phone

In addition to sending direct messages from the web, you can also send direct messages from different devices using d + username + message. (For example: d krissy I want to see that movie too; what are you doing this weekend?) Send a direct message from:

- your phone
- most 3rd party applications

Note: If your message is longer than 140 characters and Twitter receives it intact, we will send your message in two parts for you. But, beware: if your service provider breaks up long messages into two parts before sending the message to Twitter, we will only see the d+username attached to the first message! The second part will post to the public time line as a regular update because it doesn't have the d+username preceding it.

Receive direct messages when other tweets are off

You can turn phone notifications OFF and still receive Direct Twitters from followers. Here's how:

1. Log in to Twitter.
2. In the upper right hand navigation, click Settings.
3. Click the third settings tab, Mobile.
4. Use the drop down box to select Direct Messages. This means only direct messages will come to your device.

You can also do this directly from your phone. If notifications are ON, send OFF once to set your phone for direct messages only. Send OFF twice to turn on off all notifications to your phone. Haven't added your phone yet? Find more information about adding your phone here. Added your phone already? Find out what commands you can use!

Related topics

Direct Message problems/confusion
Fixed: Unable to access direct message timeline
Frequently Asked Questions
Fixed: Account settings revert to original after making changes (Username, email, password)
Account restoration does not work

Help Resources

Getting Started (42)
Using Twitter with your phone (25)
Troubleshooting (23)
Known Issues (39)
Impersonation, Trademark, and Terms of Service policies (14)
Twitter Support - jen español! (58)
Twitter Support - auf Deutsch (16)
Twitter Support - Italiano (23)
Twitter Support - en français (49)

Search

(All)

Search

Looking for information about @replies/mentions? [Click here.](#)

Help desk software by Zendesk

EXHIBIT 3

Help Resources / Getting Started / Public vs protected accounts

Public vs protected accounts

Submitted Nov 06, 2008 by crystal

Public or protected (private)?

When you sign up for Twitter, you have the option of keeping your account public (the default account setting) or protecting the account to keep your updates private. Public accounts have profile pages that are visible to everyone, and anyone can follow public updates without approval from the account owner.

Protected accounts receive a follow request each time someone wants to follow them, and only approved followers are able to see the profile page. If the idea of strangers reading your Twitter updates makes you feel a little weird, try protecting your profile at first. You can always change your mind later. Please note: **If your account is protected, we assume that you only want your followers to see your updates. @replies sent to people who aren't following you will not be seen. If you want to interact with everyone on Twitter, you should not protect your account.**

Protecting your Twitter profile

Not everyone has to see your Twitter updates. Keep your Twitter updates private and approve your followers by protecting your profile. You can protect your profile in your account settings page. Protected account owners control who is able to follow them, and keep their updates away from the public eye. Private accounts can always go public by un-checking the box in account settings.

The screenshot shows the Twitter account settings page. At the bottom, there is a checkbox labeled "Protect my updates" which is checked. Below it, a note reads: "Only let people whom I approve follow my updates. A new check is checked, you WILL NOT be on the public timeline." An arrow points to this checkbox.

To protect your profile:

1. Log in to Twitter
2. Click Settings
3. Scroll down and check the box next to "Protect my Updates"
4. SAVE your changes.

When you navigate to your home page after protecting your profile, you'll see a notice reminding you that your profile is now protected.

If I'm public and I decide to protect my profile, what happens?

If you have a public account and you protect it, all updates **after** the time of protection will be protected. Your profile will only be visible to approved followers, and existing followers will not be affected. You don't have to approve existing followers, nor do you have to follow them. You can stop sending updates to these followers at any time by clicking "remove" in your followers page. After protecting your profile, people will have to request to follow you, and each follow request will need approval. You can allow people to follow you without following them back.

When someone requests to follow me, what happens?

When someone who has requested to follow you visits your profile, they'll see a note saying "You've requested to follow this person. Remove?" until you have taken action on the follow request or the request has been canceled. Keep in mind that when you protect your profile, you:

- must approve all follow requests for people who want to receive your Twitter updates
- exclude your information from Twitter search results
- cannot share static page URLs with non-followers

If I let someone follow me, do I have to follow back?

Related topics

- Twitter search still shows updates from my private account!
- Missing mentions or replies
- Fixed: Protected Accounts' Accepted Followers aren't showing up in Followers List and Requester Can't Request Again
- Blocked/suspended users causing incorrect follow counts
- I can't access my new follower requests!

Help Resources

- Getting Started (42)
- Using Twitter with your phone (25)
- Troubleshooting (23)
- Known Issues (39)
- Impersonation, Trademark, and Terms of Service policies (14)
- Twitter Support - jen español! (58)
- Twitter Support - auf Deutsch (16)
- Twitter Support - Italiano (23)
- Twitter Support - en français (49)

Search

(All)

No. You can allow someone to follow you without following them back. If you change your mind and want to revoke follow privileges, visit your followers page, and click the remove button.

Protected/Private Profiles & Search

Please note that tweets from protected profiles will not appear in search results. People will still be able to find your account using the Find People search tool but only people you've approved to follow your account will be able to see your tweets. Also note that any tweets posted while your profile is private will remain private indefinitely, and tweets posted while your account is public will remain public indefinitely.

Help desk software by Zendesk