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