0923093

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of	)	
TWITTER, INC.,	)	
a corporation.	)	**DOCKET NO. C-**

COMPLAINT

The Federal Trade Commission, having reason to believe that Twitter, Inc. ("Twitter" or

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**

a. establish or enforce po

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 ___ day of _____, 2010, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary