092 3093

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Jon Leibowitz, Chairman**
William E. Kovacic
J. Thomas Rosch
Edith Ramirez
Ju(Ju(Ju3tl5. 00 TD(E. K)Tj(Ju8.6 0.0000 TD(E. Br11.26.3 0.0000 TD(th ill

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 any 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

IV.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federa

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the cor

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