Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Twitter, Inc., File No. 0923093

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Twitter, Inc. ("Twitter").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

Since approximately July 2006, Twitter has operated www.twitter.com, a social networking website that enables consumers who use Twitter ("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. Twitter offers privacy settings through which a user may choose to designate tweets as nonpublic. In addition, Twitter collects certain information about its users that it does not make public ("nonpublic user information"). Such information includes: an email address, Internet Protocol ("IP") addresses, 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 user information cannot be viewed by other users or any other third parties, but – with the exception of IP addresses – can be viewed after login by the account owner.

The Commission's complaint alleges that Twitter violated Section 5(a) of the FTC Act by falsely representing to consumers that it uses at least reasonable safeguards to protect user information from unauthorized access. The complaint further alleges that, through its statements regarding the privacy settings it offers to enable users to keep their tweets private, Twitter falsely represented that it maintains at least reasonable safeguards to honor the privacy choices exercised by users. Despite these representations, Twitter 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 such users in designating certain tweets as nonpublic. Specifically, Twitter failed to prevent unauthorized administrative control of the Twitter system, which includes 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. Among other things, Twitter failed 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; or (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.

The complaint alleges that between January and May 2009, intruders exploited these failures on two occasions 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 users' passwords and send unauthorized tweets from users' accounts.

The proposed order applies to "nonpublic consumer information" from or about an individual consumer. "Nonpublic consumer information" is defined broadly to 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 Twitter's microblogging platform. The proposed order contains provisions designed to prevent Twitter from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits Twitter from misrepresenting the security, privacy, confidentiality, or integrity of any "nonpublic consumer information."

Part II of the proposed order requires Twitter to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information. The security program must contain administrative, technical, and physical safeguards appropriate to Twitter's size and complexity, the nature and scope of its activities, and the sensitivity of the nonpublic consumer information. Specifically, the order requires Twitter to:

- designate an employee or employees to coordinate and be accountable for the information security program;

- identify 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 assess the sufficiency of any safeguards in place to control these risks;

- design and implement reasonable safeguards to control the risks identified through risk assessment and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures;

- develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding nonpublic consumer information they receive from respondent, and require service providers by contract to implement and maintain appropriate safeguards; and

- evaluate and adjust its information security program in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on the effectiveness of its information security program.

Part III of the proposed order requires that Twitter obtain within 180 days, and on a biennial basis thereafter for ten (10) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: it has in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed order; and its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, privacy, confidentiality, and integrity of nonpublic consumer information is protected.

Parts IV through VIII of the proposed order are reporting and compliance provisions. The proposed order requires Twitter to retain for a period of five (5) years from the date received, documents that contradict, qualify, or call into question its compliance with this order. Part IV further requires that Twitter retain all materials relied upon to prepare the third-party assessments for a period of three (3) years after the date that each assessment is prepared. In addition, Part IV requires that Twitter retain all "widely-disseminated statements" that describe the extent to which it maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information, along with all materials relied upon in making or disseminating such statements, for a period of three (3) years after the date of preparation or dissemination, whichever is later. Part IV also requires Twitter to maintain for six (6) months from the date received all consumer complaints directed at Twitter or forwarded to Twitter from a third party that relate to the activities alleged in the proposed complaint. Finally, Part IV requires that Twitter maintain for two (2) years from the date received copies of all subpoenas and communications with law enforcement, if such communications relate to Twitter's compliance with the order.

Part V requires dissemination of the order now and in the future to principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that Twitter submit an initial compliance report to the FTC and make available to the FTC subsequent reports. Part VIII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of the analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order or to modify its terms in any way.