

Complaint

**IN THE MATTER OF
TWITTER, INC.****CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT**

*Docket No. C-4316; File No. 092 3093
Filed March 2, 2011 – Decision March 2, 2011*

This consent order relates to allegations that Twitter, Inc. (“Twitter”), a social networking website that enables users to send brief messages of 140 characters or less to others, falsely represented to consumers that it honored users’ privacy choices and that used reasonable and appropriate safeguards to protect nonpublic user information from unauthorized access, in violation of Section 5 of the FTC Act. The consent order prohibits Twitter from misrepresenting the security, privacy, confidentiality, or integrity of any “nonpublic consumer information.” The order requires Twitter to establish and maintain a comprehensive information security program that is designed to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information. The consent order also requires Twitter to establish, and on a biennial basis thereafter for ten years, an assessment and report from a qualified, objective, independent third-party professional certifying that it has in place a security program that provides reasonable assurance that the security, privacy, confidentiality, and integrity of nonpublic consumer information is protected.

Participants

For the Commission: *Laura D. Berger, Cora Tung Han, Maneesha Mithal, and Christopher Olsen.*

For the Respondent: *Alexander MacGillivray, Twitter, Inc.; Lydia Parnes, Wilson Sonsini Goodrich & Rosati.*

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:

Complaint

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”

Complaint

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.

Complaint

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

Complaint

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

Complaint

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

Complaint

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.

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.

Decision and Order

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

Decision and Order

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.

Decision and Order

- 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

Decision and Order

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;

Decision and Order

- 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;

Decision and Order

- 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.

Decision and Order

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:

Decision and Order

- 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.

ANALYSIS OF PROPOSED CONSENT ORDER TO AID PUBLIC COMMENT

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

Analysis to Aid Public Comment

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 –

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Complaint

**IN THE MATTER OF
US SEARCH, INC. AND US SEARCH, LLC****CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT**

*Docket No. C-4317; File No. 102 3131
Filed March 14, 2011 – Decision March 14, 2011*

This consent order addresses allegations that US Search, Inc. and US Search, LLC (collectively “US Search”) engaged in deceptive acts or practices, in violation of Section 5 of the FTC Act, by misrepresenting that the purchase or use of its PrivacyLock service would prevent a consumer’s name and address from appearing on US Search’s website, in its advertisements, or in its search results. US Search, who operates an online data broker service, sells publicly available information about consumers to other consumers through its website, www.ussearch.com. This publicly available information includes a consumer’s name, age, address, phone numbers, email addresses, aliases, maiden name, death records, address history, information about friends, associates, and relatives, marriage and divorce information, bankruptcies, tax liens, civil lawsuits, criminal records, and home values. The consent order includes injunctive relief that enjoins US Search from misrepresenting the effectiveness of its PrivacyLock service or any other service offered to consumers that will allow consumers to remove publicly available information from US Search’s search results, websites, and advertisements. The order also requires US Search to refund any money consumers paid for the PrivacyLock service. Under the proposed order, US Search must credit consumers’ credit and debit card accounts and notify consumers via email that such credits were made.

Participants

For the *Commission*: Amanda Koulousias and Anthony Rodriguez.

For the *Respondents*: Becky Burr, WilmerHale.

COMPLAINT

The Federal Trade Commission, having reason to believe that US Search, Inc., a corporation, and US Search, LLC, a limited liability