

Complaint

IN THE MATTER OF

CREDIT KARMA, INC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4480; File No. 132 3091
Complaint, August 13, 2014 – Decision, August 13, 2014

This consent order addresses Credit Karma, Inc.'s security for its website and mobile application that allow consumers to monitor and evaluate their credit and financial status. The complaint alleges that Credit Karma engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security in the development and maintenance of its mobile application. The complaint further alleges that, due to these failures, attackers could, in connection with attacks that redirect and intercept network traffic, decrypt, monitor, or alter any of the information transmitted from or to the application, including Social Security numbers, dates of birth, "out of wallet" information, and credit report information. The consent order requires Credit Karma to (1) address security risks related to the development and management of new and existing products and services for consumers, and (2) protect the security, integrity, and confidentiality of covered information, whether collected by Credit Karma or input into, stored on, captured with, or accessed through a computer using Credit Karma's products or services. The order also prohibits Credit Karma from misrepresenting the extent to which Credit Karma or its products or services maintain and protect the privacy, security, confidentiality, or integrity of covered information.

Participants

For the *Commission*: Jarad Brown and Nithan Sannappa.

For the *Respondent*: Reed Freeman, Morrison & Foerster LLP.

COMPLAINT

The Federal Trade Commission, having reason to believe that Credit Karma, Inc. ("respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

Complaint

1. Respondent Credit Karma, Inc. (“Credit Karma”) is a Delaware corporation with its principal office or place of business at 115 Sansome Street, Suite 400, San Francisco, CA 94104.

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 Federal Trade Commission Act.

RESPONDENT’S BUSINESS PRACTICES

3. Credit Karma provides a website and mobile application that allow consumers to monitor and evaluate their credit and financial status. Credit Karma allows consumers to access credit scores and credit reports, and a “Credit Report Card” summarizing key credit report metrics, and also offers credit monitoring.

4. The Credit Karma Mobile application – available for Apple, Inc.’s iOS operating system since July 2012 and Google, Inc.’s Android operating system since February 2013 – allows consumers to access their credit score, monitor their credit score history, access their “Credit Report Card,” access a summary of the accounts on their credit report, including specific account names and balances, and obtain notifications regarding significant changes in their credit report.

5. Both the iTunes App Store and the Google Play Store list Credit Karma Mobile among the top 10 free applications in the Finance category. The application has been downloaded over one million times.

6. When a consumer creates an account through the Credit Karma Mobile application, the application transmits sensitive personal information to Credit Karma, including the consumer’s email address, password, security question and answer, first name, last name, date of birth, street address, apartment number, city, zip code, phone number, and Social Security Number. During the account creation process, the application also transmits the consumer’s answers to “out of wallet” questions, which are multiple choice questions validating the consumer’s identity (e.g., questions about a past mortgage provider or the payment amount on a loan).

Complaint

7. Credit Karma outsourced the software development of both the iOS and Android versions of the Credit Karma Mobile application to application development firms that acted as its service providers and agreed to certain product security requirements.

**SECURE SOCKETS LAYER CERTIFICATE
VALIDATION**

8. Consumers frequently use mobile applications on public Wi-Fi networks in venues such as coffee shops, shopping centers, and airports. Consumers may use the Credit Karma Mobile application in such public environments. Indeed, Credit Karma marketed Credit Karma Mobile on the iTunes App Store and the Google Play Store as a way for consumers to get “free on-the-go credit monitoring.”

9. Online services often use the Secure Sockets Layer (“SSL”) protocol to establish authentic, encrypted connections with consumers. In order to authenticate and encrypt connections, SSL relies on electronic documents called SSL certificates.

10. In the context of mobile applications, an online service (*e.g.*, Credit Karma) presents an SSL certificate to the application on a consumer’s device (*e.g.*, Credit Karma Mobile) to vouch for its identity. The application must then validate the SSL certificate – in effect verifying the identity of the online service – to ensure that the application is connecting to the genuine online service. After completing this process, the online service and the application on the consumer’s device can establish a secure connection that is both authenticated and encrypted.

11. If the application fails to perform this process, an attacker could position himself between the application on the consumer’s device and the online service by presenting an invalid certificate to the application. The application would accept the invalid certificate and establish a connection between the application and the attacker, allowing the attacker to decrypt, monitor, or alter all communications between the application and the online service. This type of attack is known as a “man-in-the-middle attack.” Neither the consumer using the application nor the online service could feasibly detect the attacker’s presence.

Complaint

12. On many public Wi-Fi networks, attackers can use well-known spoofing techniques to facilitate man-in-the-middle attacks.

13. To protect against these attacks, the iOS and Android operating systems provide developers with application programming interfaces (“APIs”) that allow applications to create secure connections using SSL. By default, these APIs validate SSL certificates and reject the connection if the SSL certificate presented to the application is invalid.

14. The developer documentation for both iOS and Android warns developers against disabling the default validation settings or otherwise failing to validate SSL certificates. The iOS documentation explains that failing to validate SSL certificates “eliminates any benefit you might otherwise have gotten from using a secure connection. The resulting connection is no safer than sending the request via unencrypted HTTP because it provides no protection from spoofing by a fake server.” Similarly, the Android documentation states that an application that does not validate SSL certificates “might as well not be encrypting [the] communication, because anyone can attack [the application’s] users at a public Wi-Fi hotspot . . . [and] the attacker can then record passwords and other personal data.”

15. Application developers can easily test for and identify SSL certificate validation vulnerabilities using free or low-cost, publicly available tools.

CREDIT KARMA’S SECURITY FAILURES

16. From July 18, 2012 to January 2013, the Credit Karma Mobile application for iOS failed to validate SSL certificates, overriding the defaults provided by the iOS APIs. On or around January 1, 2013, a Credit Karma user informed respondent that its iOS application was vulnerable to man-in-the-middle attacks because it did not validate SSL certificates. Respondent’s in-house security engineers issued an update to the application in January 2013 that enabled SSL certificate validation by restoring the iOS API default settings.

Complaint

17. During the iOS application's development, Credit Karma had authorized its service provider, the application development firm, to use code that disabled SSL certificate validation "in testing only," but failed to ensure this code's removal from the production version of the application. As a result, the iOS application shipped to consumers with the SSL certificate validation vulnerability. Credit Karma could have identified and prevented this vulnerability by performing an adequate security review prior to the iOS application's launch. In February 2013, one month after addressing the vulnerability in its iOS application, Credit Karma launched the Android version of its application, again without first performing an adequate security review or at least testing the application for previously identified vulnerabilities. As a result, like the iOS application before it, the Android application failed to validate SSL certificates, overriding the defaults provided by the Android APIs.

18. Credit Karma did not perform an adequate security review of the Credit Karma Mobile application until after Commission staff contacted respondent. At that time, Credit Karma's in-house security team performed a basic, low-cost security review of both the iOS and Android versions of the application over the course of several hours.

19. Through the security review, respondent discovered that its service provider had introduced the same SSL certificate validation vulnerability into its Android application that respondent had been warned about and remedied in its iOS application just one month earlier. Respondent issued an update to the Android application in March 2013, enabling SSL certificate validation by restoring the Android API default settings. Credit Karma could have prevented the re-introduction of this vulnerability in the Android version of its application had it performed an adequate security review prior to launch or at least tested the application for previously identified vulnerabilities.

20. Through the security review, respondent's in-house security team also discovered that the iOS application was storing authentication tokens and passcodes on the device in an insecure manner, contrary to security requirements that the application development firm had agreed to implement (*i.e.*, encrypting this information with the "keychain" API provided by the iOS

Complaint

operating system). Credit Karma could have ensured the implementation of its product security requirements by providing reasonable oversight of its service providers during the development process and performing an adequate security review of its application prior to launch.

21. Respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security in the development and maintenance of its mobile application, including:

- a. Overriding the default SSL certificate validation settings provided by the iOS and Android APIs without implementing other security measures to compensate for the lack of SSL certificate validation;
- b. Failing to appropriately test, audit, assess, or review its applications, including failing to ensure that the transmission of sensitive personal information was secure; and
- c. Failing to reasonably and appropriately oversee its service providers' security practices.

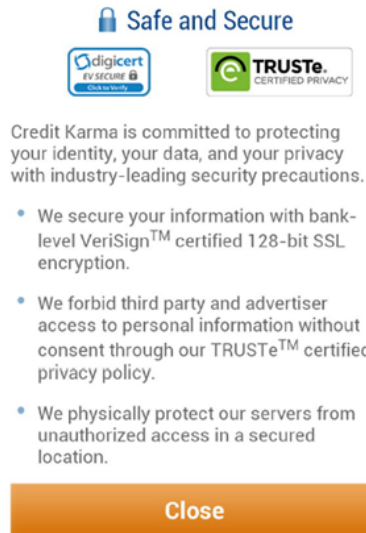
22. As a result of these failures, attackers could, in connection with attacks that redirect and intercept network traffic, decrypt, monitor, or alter any of the information transmitted from or to the application, including Social Security numbers, dates of birth, "out of wallet" information, and credit report information. Attackers also could intercept a consumer's authentication credentials, allowing an attacker to log into the consumer's Credit Karma web account to access the consumer's credit score and a more complete version of the consumer's credit report. The misuse of these types of sensitive personal information can lead to identity theft, including existing and new account fraud, the compromise of personal information maintained on other online services, and related consumer harms.

23. Credit Karma could have prevented these vulnerabilities and ensured the secure transmission of consumers' sensitive personal information by performing basic, low-cost security reviews, such as the one described in paragraph 18.

Complaint

CREDIT KARMA'S PRIVACY AND SECURITY REPRESENTATIONS

24. Since the launch of the Credit Karma Mobile application on iOS and Android, Credit Karma disseminated or caused to be disseminated to consumers the following in-app representation when a consumer created an account using the application:



25. Since at least the launch of the Credit Karma Mobile application on iOS and Android, Credit Karma disseminated or caused to be disseminated to consumers the following representation in its privacy policy:

We enable our servers with Secure Socket Layer (SSL) technology to establish a secure connection between your computer and our servers, creating a private session.

**CREDIT KARMA'S DECEPTIVE REPRESENTATIONS
(Count 1)**

26. As described in Paragraph 24, Credit Karma has represented, expressly or by implication, that it is committed to protecting Credit Karma Mobile application users' identity, data, and privacy with reasonable and appropriate security practices.

Decision and Order

27. In truth and in fact, as set forth in Paragraphs 16 – 23, Credit Karma failed to protect Credit Karma Mobile application users' identity, data, and privacy with reasonable and appropriate security practices. Therefore, the representation set forth in Paragraph 26 was false or misleading.

(Count 2)

28. As described in Paragraphs 24 and 25, Credit Karma has represented, expressly or by implication, that the Credit Karma Mobile application transmits consumers' sensitive personal information over secure SSL connections.

29. In truth and in fact, as set forth in Paragraphs 8 – 19, the Credit Karma Mobile application did not transmit consumers' sensitive personal information over secure SSL connections. Therefore, the representation set forth in Paragraph 28 was false or misleading.

30. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this thirteenth day of August, 2014, has issued this complaint against respondent.

By the Commission, Commissioner McSweeney not participating.

DECISION AND ORDER

The Federal Trade Commission ("Commission" or "FTC"), 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

Decision and Order

that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45 *et seq.*;

The respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; 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 had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such 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 pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, now in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Order:

1. Respondent Credit Karma, Inc. (“Credit Karma”) is a Delaware corporation with its principal office or place of business at 115 Sansome Street, Suite 400, San Francisco, CA 94104.
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.

Decision and Order

ORDER**DEFINITIONS**

For purposes of this order, the following definitions shall apply:

- A. Unless otherwise specified, “respondent” shall mean Credit Karma, Inc. and its successors and assigns.
- B. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
- C. “Covered information” shall mean information from or about an individual consumer, including but not limited to (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other state-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) credit report information; (j) a persistent identifier, such as a customer number held in a “cookie,” a static Internet Protocol (“IP”) address, a mobile device ID, or processor serial number; (k) precise geo-location data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information; (l) an authentication credential, such as a username or password; or (m) any communications or content that is input into, stored on, captured with, or accessed through a computer, including but not limited to contacts, emails, SMS messages, photos, videos, and audio recordings.
- D. “Computer” shall mean any desktop, laptop computer, tablet, handheld device, telephone, or other electronic product or device that has a platform on which to download, install, or run any software program, code, script, or other content and to play any digital audio, visual, or audiovisual content.

Decision and Order

- E. “Client software” shall mean any program or application developed by respondent or any corporation, subsidiary, division, or affiliate owned or controlled by respondent, that is installed locally on a consumer’s computer and that communicates with a server.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent, shall not misrepresent in any manner, expressly or by implication, the extent to which respondent or its products or services maintain and protect the privacy, security, confidentiality, or integrity of any covered information.

II.

IT IS FURTHER ORDERED that respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing products and services for consumers, and (2) protect the security, integrity, and confidentiality of covered information, whether collected by respondent or input into, stored on, captured with, or accessed through a computer using respondent’s products or services. 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 covered information, including:

- A. the designation of an employee or employees to coordinate and be accountable for the security program;
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized

Decision and Order

disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent's possession or is input into, stored on, captured with, or accessed through a computer using respondent's products or services, and assessment of the sufficiency of any safeguards in place to control these risks.

- C. at a minimum, the risk assessment required by Subpart B should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development and research; (3) secure software design, development, and testing; (4) review, assessment, and response to third-party security vulnerability reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures;
- D. 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, including through reasonable and appropriate software security testing techniques;
- E. the development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards;
- F. the evaluation and adjustment of respondent's security program in light of the results of the testing and monitoring required by subpart B, 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 security program.

Decision and Order

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, for any product or service offered through client software, 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 Secure Software Lifecycle Professional (CSSLP) with experience in secure mobile programming; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and secure mobile programming; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific controls and procedures 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 covered information;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and
- D. certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of covered information is protected and has so operated throughout the reporting period.

Decision and Order

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. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of Credit Karma, Inc.*, FTC File No. 1323091. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

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 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, and any other materials relating to respondent's compliance with Parts II and III of this order, for the compliance period covered by such Assessment;
- B. unless covered by IV.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all other documents relating to

Decision and Order

compliance with this order, including but not limited to:

1. all advertisements and promotional materials containing any representations covered by this order, as well as all materials used or relied upon in making or disseminating the representation; and
2. any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order.

V.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure. Respondent must secure a signed and dated statement acknowledging receipt of this order, within thirty (30) days of delivery, from all persons receiving a copy of the order pursuant to this section.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) 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 the corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty

Decision and Order

(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. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of Credit Karma, Inc.*, FTC File No. 1323091. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VII.

IT IS FURTHER ORDERED that respondent, within one hundred twenty (120) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit an additional true and accurate written report.

VIII.

This order will terminate on August 13, 2034, 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:

- A. any Part in this order that terminates in fewer than twenty (20) years;
- B. this order's application to any respondent that is not named as a defendant in such complaint; and
- C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Analysis to Aid Public Comment

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, Commissioner McSweeney not participating.

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission has accepted, subject to final approval, a consent order applicable to Credit Karma, Inc. (“Credit Karma”).

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.

Credit Karma operates a website and mobile application that allow consumers to monitor and evaluate their credit and financial status. Through its service, consumers can access their credit scores, credit reports, a “Credit Report Card” summarizing key credit report metrics, and obtain credit monitoring.

The Commission’s complaint alleges that Credit Karma deceived consumers regarding its commitment to industry-leading security practices and its transmission of consumers’ sensitive

Analysis to Aid Public Comment

personal information over secure connections. Specifically, the complaint alleges that Credit Karma engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security in the development and maintenance of its mobile application, including:

- (1) overriding the mobile operating system default settings that would have secured the transmission of sensitive personal information to and from the mobile application;
- (2) failing to appropriately test, audit, assess, or review its applications, including failing to ensure that the transmission of sensitive personal information was secure; and
- (3) failing to reasonably and appropriately oversee its service providers' security practices.

The complaint further alleges that, due to these failures, attackers could, in connection with attacks that redirect and intercept network traffic, decrypt, monitor, or alter any of the information transmitted from or to the application, including Social Security numbers, dates of birth, "out of wallet" information, and credit report information. The complaint also alleges that attackers could intercept a consumer's authentication credentials, allowing an attacker to log into the consumer's Credit Karma web account to access the consumer's credit score and a more complete version of the consumer's credit report. The complaint alleges that the misuse of these types of sensitive personal information can lead to identity theft including existing and new account fraud, the compromise of personal information maintained on other online services, and related consumer harms.

The proposed order contains provisions designed to prevent Credit Karma from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits Credit Karma from misrepresenting the extent to which Credit Karma or its products or services maintain and protect the privacy, security, confidentiality, or integrity of covered information. Part II of the proposed order requires Credit Karma to (1) address security risks

Analysis to Aid Public Comment

related to the development and management of new and existing products and services for consumers, and (2) protect the security, integrity, and confidentiality of covered information, whether collected by Credit Karma or input into, stored on, captured with, or accessed through a computer using Credit Karma's products or services. The security program must contain administrative, technical, and physical safeguards appropriate to Credit Karma's size and complexity, nature and scope of its activities, and the sensitivity of the covered information. Specifically, the proposed order requires Credit Karma to:

- designate an employee or employees to coordinate and be accountable for the information security program;
- identify material internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in Credit Karma's possession or is input into, stored on, captured with, accessed or transmitted through a computer using Credit Karma's products or services, and assess the sufficiency of any safeguards in place to control these risks;
- consider risks in each area of relevant operation, including but not limited to (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development and research; (3) secure software design, development, and testing; and (4) review, assessment, and response to third-party security vulnerability reports; and (5) prevention, detection, and response to attacks, intrusions, or system failures;
- 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, including through reasonable and appropriate software security testing techniques;

Analysis to Aid Public Comment

- develop and use reasonable steps to select and retain service providers capable of maintaining security practices consistent with the order, and require service providers by contract to implement and maintain appropriate safeguards; and
- evaluate and adjust its security program in light of the results of testing and monitoring, any material changes to Credit Karma's operations or business arrangement, or any other circumstances that it knows or has reason to know may have a material impact on the effectiveness of its security program.

Part III of the proposed order requires Credit Karma to obtain, for any product or service offered through client software, within the first one hundred eighty (180) days after service of the order and on a biennial basis thereafter for a period of twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) 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 (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of covered information is protected.

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires Credit Karma to retain documents relating to its compliance with the order. The order requires that all materials relied upon to prepare the assessments required by Part III of the order be retained for a three-year period, and that other documents, such as advertisements and promotional materials covered by the order, be retained for a five-year period. Part V requires dissemination of the order to all current and future subsidiaries, current and future principals, officers, directors, and managers having responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII requires Credit Karma to submit a compliance report to the FTC within 120 days, and periodically thereafter as requested. Part VIII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

Analysis to Aid Public Comment

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed complaint or order or to modify the order's terms in any way.

Complaint

IN THE MATTER OF

GMR TRANSCRIPTION SERVICES, INC.;
AJAY PRASAD;
AND
SHREEKANT SRIVASTAVACONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4482; File No. 122 3095
Complaint, August 14, 2014 – Decision, August 14, 2014

This consent order GMR Transcription Services, Inc.'s practices to protect consumers' personal information from unauthorized access. The complaint alleges that engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for consumers' personal information. The complaint further alleges that as a result of these security failures files were publicly available, and were accessed, using a major search engine. The consent order requires respondents to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The order also prohibits respondents from misrepresenting the extent to which respondents use, maintain, and protect the privacy, confidentiality, security, or integrity of personal information collected from or about consumers.

Participants

For the *Commission*: Kandi Parsons and Alain Sheer.

For the *Respondents*: Barry Coburn, Kimberly Jandrain, Lloyd Lui, and Monica Seaman, Coburn & Greenbaum PLLC.

COMPLAINT

The Federal Trade Commission, having reason to believe that GMR Transcription Services, Inc., Ajay Prasad, and Shreekant Srivastava have violated the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges: