

**UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION**

In the Matter of	)	
	)	<b>AGREEMENT CONTAINING</b>
	)	<b>CONSENT ORDER</b>
Credit Karma, Inc.,	)	
a corporation.	)	
	)	<b>FILE NO. 132 3091</b>

The Federal Trade Commission (“Commission”) has conducted an investigation of certain acts and practices of Credit Karma, Inc. (“Credit Karma” or “proposed respondent”). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

**IT IS HEREBY AGREED** by and between Credit Karma, Inc., by its duly authorized officers, and counsel for the Federal Trade Commission that:

1. Proposed respondent Credit Karma, Inc. is a Delaware corporation with its principal office or place of business at 115 Sansome Street, Suite 400, San Francisco, CA 94104.
2. Proposed respondent admits all jurisdictional facts set forth in the draft complaint.
3. Proposed respondent waives:
  - A. any further procedural steps;
  - B. the requirement that the Commission’s decision contain a statement of findings of fact and conclusions of law; and
  - C. all rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.
4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.
6. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to proposed respondent, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent's address as stated in this agreement by any means specified in Section 4.4(a) of the Commission's Rules shall constitute service. Proposed respondent waives any right it may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or the agreement may be used to vary or contradict the terms of the order.
7. Proposed respondent has read the draft complaint and consent order. Proposed respondent understands that it may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

## ORDER

### DEFINITIONS

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

1. "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.

2. “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.
3. “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.
4. Unless otherwise specified, “respondent” shall mean Credit Karma, Inc. and its successors and assigns.
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 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 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.

### 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.

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](mailto: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 compliance with this order, including but not limited to:

- i. 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
- ii. 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 (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](mailto: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 twenty (20) years from the date of its issuance, 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.

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.

Signed this \_\_\_\_\_ day of \_\_\_\_\_, 2013.

CREDIT KARMA, Inc.

Dated: \_\_\_\_\_

By: \_\_\_\_\_  
KENNETH LIN, Chief Executive Officer  
Credit Karma, Inc.

Dated: \_\_\_\_\_

By: \_\_\_\_\_  
D. REED FREEMAN JR., Esq.  
Morrison & Foerster, LLP  
2000 Pennsylvania Ave., N.W., Suite 6000  
Washington, DC 20006  
Attorney for Respondent

FEDERAL TRADE COMMISSION

Dated: \_\_\_\_\_

By: \_\_\_\_\_  
NITHAN SANNAPPA  
Counsel for the Federal Trade Commission

APPROVED:

\_\_\_\_\_  
MARK EICHORN  
Assistant Director  
Division of Privacy and Identity Protection

\_\_\_\_\_  
MANEESHA MITHAL  
Associate Director  
Division of Privacy and Identity Protection

\_\_\_\_\_  
JESSICA RICH  
Director  
Bureau of Consumer Protection