

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Edith Ramirez, Chairwoman**
 Julie Brill
 Maureen K. Ohlhausen
 Joshua D. Wright
 Terrell McSweeney

)	
In the Matter of)	
)	DOCKET No. C-4480
Credit Karma, Inc.)	
)	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 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 waives 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.

ORDER

DEFINITIONS

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

1. Unless otherwise specified, “respondent” shall mean Credit Karma, Inc. and its successors and assigns.
2. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
3. “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.
4. “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.
5. “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

- 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.

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

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,

- A. any Part in this order that terminates in fewer than twenty (20) years;
- B.