

**Analysis of Proposed Consent Order to Aid Public Comment**  
***In the Matter of Credit Karma, Inc., File No. 132 3091***

---

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 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 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;
- 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.

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.