In the Matter of	)	**DOCKET NO. C-4480**
Credit Karma, Inc.,	)	
a corporation.	)	**appearing to the Commission that this proceeding is in the pub**

1. Respondent Credit Karma, Inc. ("Credit Karma") is a Delaw
principal office or place of business at 115 Sansome Street,
94104.
2. The acts and practices of respondent as alleged in this co

RESPONDENT'S BUSINESS PRACT

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.

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

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 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, decrnd

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 ecofndne-Afer(sm)9s’ 0.001-2(sen)60fnd e-t(e)nd e-vsmesmde-ofndnby-2(s)-1(ona)(m)8(a)-1(t)-21(d ong)15 T1

(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 McSweeny not participating.

Donald S. Clark
Secretary