JENNER&BLOCK

April 1, 2014

Privacy and Information Governance

FTC Ratchets Up Data Security Standards Obligations for Mobile App Developers

By Mary Ellen Callahan and Sabrina N. Guenther

On March 28, 2014, the Federal Trade Commission announced settlements with two mobile app developers who allegedly failed to implement reasonable and appropriate data security measures in the development and maintenance of their mobile apps. The allegations—specifically, that the app developers did not employ default security measures or sufficient replacement measures and that the developers had misrepresented the security of their apps—offer further insight into what the FTC considers reasonable data security standards regarding mobile apps. In particular, the FTC signaled in the draft complaint against one of the app developers, Credit Karma, Inc. (Credit Karma), that it will hold app developers responsible for some failures of their third-party service providers, even where those third-party service providers had contractually agreed to implement certain security features. The FTC complaints against both developers, Credit Karma and Fandango LLC (Fandango), also relied on the standards and warnings set out in mobile operating systems' application programming interfaces (APIs) as evidence of reasonable and available data security and privacy measures and industry standards.

These cases drive home the importance of diligent monitoring and auditing for the security of mobile apps. App developers should assess the security measures they use, the testing they conduct, and the supervision they conduct of third-party service providers. They also should analyze the APIs that apply to their apps and proceed cautiously if they decide to deviate from the defaults and recommendations therein.

Complaints and Consent Decrees

Fandango and Credit Karma both offer popular mobile apps. Fandango's app, which operates only on iOS (Apple's platform), allows consumers to purchase movie tickets from the app. To complete the transaction, the app collects, stores and transfers consumers' credit card information, including card number, security code, expiration date, billing ZIP code and some consumers' email addresses and passwords. Credit Karma's apps on both iOS and Android (Google's platform) allow consumers to access credit scores and reports and to monitor their credit. When consumers create their accounts, the app transmits their email addresses, passwords, security questions and answers, names, birthdates, street addresses, cities, ZIP codes, phone numbers, Social Security numbers and consumers' responses to identity questions (e.g., about past mortgages or loans, etc.).

Fandango developed the software for its own app, while Credit Karma had outsourced its software development to third-party service providers. In their contracts with Credit Karma, those firms agreed to implement certain product security requirements.

The FTC alleged that both Fandango and Credit Karma failed to implement Secure Socket Layer (SSL) certificate verification to authenticate and encrypt consumers' sensitive personal information. As a result, consumers' information was left vulnerable to man-in-the-middle attacks, though the FTC did not allege that any such attacks occurred. Both iOS and Android provide SSL technology to their app developers as a default security measure for in-app transactions, and both recommend against disabling SSL verification.

The FTC did not allege that either Fandango or Credit Karma knowingly opted out of the default SSL settings for their applications when released publicly, rather that each failed to appropriately test the data security of their apps. Fandango limited its security audits to identify only some data security errors, but within three weeks of hearing from the FTC, Fandango engaged in more extensive testing and issued a security update to consumers to fix the error. Credit Karma allowed its third-party service providers to test software with SSL disabled and then failed to ensure the production version of its app included the SSL features. While Credit Karma discovered and fixed this issue in its iOS app in January 2013, it released an Android app with same deficiency a month later. Furthermore, per the FTC, Credit Karma discovered another security issue in it iOS app only after the FTC had reached out regarding its concerns.

The FTC concluded both complaints by alleging that Fandango and Credit Karma had violated Section 5(a) of the Federal Trade Commission Act by engaging in unfair or deceptive trade practices. In the complaint against Fandango, the FTC did not include any counts specifying an unfair or deceptive trade practice. The complaint against Credit Karma included two specific counts of deception.

The consent decrees require Fandango and Credit Karma not to misrepresent their privacy and security practices, to establish comprehensive security programs (including accountable employees, regular testing and monitoring, selection and use of service providers capable of maintaining and implementing the same safeguards), and to submit to 20 years of biennial assessments and reports, among other administrative requirements.

Oversight of Third Parties and Security Standards

As discussed above, the FTC's allegations against Fandango and Credit Karma were largely similar. Both included allegations about the popularity of the apps and the deficiency of the app developers' data security testing. Also, in each complaint, the FTC alleged that the app developer failed to follow the iOS and Android developer materials, including the APIs and the recommendations regarding disabling SSL security measures. These allegations demonstrate not only that the FTC has focused on the content of the APIs, but also that it may see them as *de facto* evidence of reasonable or industry standard data security and privacy practices. In addition, the FTC's allegations regarding the insufficient security testing, even in response to consumer and regulatory complaints, demonstrate the risks of taking shortcuts in auditing. App developers should diligently review app security, especially in cases like these, where the apps involve sensitive consumer information such as credit card information and Social Security numbers.

Nonetheless, at least one significant difference remained between the allegations against Fandango versus those against Credit Karma—Credit Karma's use of third-party software developers. Whereas Fandango had introduced the security vulnerabilities into its own app, the third-party developers were responsible for the data security features in Credit Karma's app. Even so, the FTC took the position that "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." Importantly, according to the FTC, Credit Karma bears responsibility even though the third-parties had contractually agreed to implement certain security features. Merely placing contractual responsibility for data security features on a third party will not protect an app developer from liability where it failed to supervise the third party and audit its product. Thus, app developers must thoroughly supervise third-party service providers and their work product or risk responsibility for the failures of those third parties.

Despite the (albeit limited) differences in the allegations, the consent decrees reached with Fandango and Credit Karma were nearly identical. Their requirements—that the app developers establish comprehensive security programs, abide by those programs and submit to reviews and reports of those programs for 20 years — are the standard requirements for FTC security consent decrees and demonstrate that the FTC focused not only on the developers' statements to consumers that it alleged were deceptive, but also on the developers' failures as unfair data security practices.

Conclusion

The Fandango and Credit Karma actions highlight important steps for those involved in developing mobile apps. In light of these consent decrees, companies should consider:

- the security measures used in their mobile apps, including whether the application has deviated from platform recommended security standards;
- the frequency and scope of any security testing they conduct;

- what types of tasks and obligations they have outsourced to third-party service providers;
- how closely they monitor any third-party service providers; and
- generally their compliance with the APIs applicable to their mobile apps.

As companies consider these issues, they may want to formalize their conclusions and evaluate how best to systematize data security development and audit controls.

Contact Us

Mary Ellen Callahan, Partner, Jenner & Block

Phone: 202.639.6064 Email: mecallahan@jenner.com DOWNLOAD V-CARD

Practices: Privacy and Information Governance; Content, Media & Entertainment; Litigation

Sabrina N. Guenther, Associate, Jenner & Block

Phone: 312.840.7299 Email: sguenther@jenner.com DOWNLOAD V-CARD

Practices: Privacy and Information Governance; Litigation

Under professional rules, this communication may be considered advertising material. The material contained in this document has been authored or gathered by Jenner & Block for informational purposes only. It is not intended to be and is not considered to be legal advice. Transmission is not intended to create and receipt does not establish an attorney-client relationship. Legal advice of any nature should be sought from legal counsel. Tax Matters: To the extent this material or any attachment concerns tax matters, it is not intended or written to be used, and cannot be used by a taxpayer, for the purpose of avoiding penalties that may be imposed on the taxpayer under law.