Privacy & Security

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Privacy & Security Alert

APRIL 3, 2014

Stop Phoning It in on Mobile Security: What Your Business Needs to Know About the FTC’s Settlements with Fandango and Credit Karma

BY CYNTHIA LAROSE, CIPP AND JAKE ROMERO, CIPP

If you’re like most Americans, you probably think that the worst thing that Fandango, the online movie ticket service, has ever done to you is make you watch those commercials with the creepy talking paper bags before your movie. The Federal Trade Commission (FTC), however, begs to differ.

According to an FTC press release, Fandango, LLC and Credit Karma, Inc., a credit information company, have agreed to settle charges brought by the FTC alleging that the companies misrepresented the security provided to users of their respective mobile applications and failed to secure the transmissions of millions of users who provided personal information through the applications. The central allegation in both complaints is that Fandango and Credit Karma failed to properly implement and utilize SSL protocols to validate exchanges of information.

How SSL Protocols Protect Users of Online Services

SSL, which stands for “Secure Sockets Layer,” is a protocol used in online transactions to establish authentic, encrypted connections between two parties. To do this, SSL requires electronic validations (referred to as “SSL certificates”) to verify the identity of the parties. If the certificates cannot be verified, SSL refuses to make the connection. On your mobile phone, the way this works is that an online service provider (such as a mobile application) presents its certificate to the application on your device. If the verification checks out, then a secure connection is established and information can be exchanged. The SSL protocol is important because without it transmissions made on public Wi-Fi networks are susceptible to what are referred to as “man-in-the-middle-attacks,” where an attacker positions himself between the user and the online service by presenting an invalid certificate so that they can monitor and intercept the unencrypted exchange of potentially personal information between the two parties. To prevent this type of attack from occurring, operating systems provide mobile application developers with application program interfaces (APIs) that, by default, refuse to establish an SSL connection if a certificate is invalid. Developer documentation for both iOS and Android platforms also provides warnings against disabling or circumventing this feature.

Allegations Against Credit Karma

In its complaint against Credit Karma, the FTC alleges that in separate incidents Credit Karma’s mobile application for iOS and Android were launched to consumers with code that disabled SSL validation and overrode the defaults provided by the platform APIs. In one case, the code had been implemented with Credit Karma’s authorization by a third-party developer during the application’s testing phase, but remained in the application following release to the general public. According to the FTC, these two errors were not detected and addressed until after Credit Karma was contacted by a user and the FTC and made aware of the vulnerability. During an internal security review conducted thereafter, Credit Karma discovered that its iOS application was storing authentication tokens and passcodes on the device in an insecure manner. The FTC alleges that Credit Karma (a) overrode the default SSL certificate validation settings without implementing other security measures to compensate, (b) failed to appropriately test, audit, assess, or review its application, and (c) failed to appropriately oversee its service providers' security practices.

Allegations Against Fandango

As of August 2013, approximately 20% of tickets purchased from Fandango have been from its mobile application. As in the complaint against Credit Karma, the claims alleged by the FTC against Fandango are focused on failures relating to both implementation and testing. In Fandango's case, its Fandango Movies application failed to validate SSL certificates for 4 years following the launch of the application in March 2009. According to the FTC, Fandango commissioned security audits starting in 2011, but those audits were limited in scope and did not include a review of the security of the application's transmission of information. Moreover, Fandango did not implement an effective channel for security complaints, and instead relied on its general customer service system to handle security vulnerability reports. In one case, the automated system failed to identify a security researcher's warning message about the security gap and assumed the individual needed help resetting his password. The FTC alleges that Fandango (a) overrode the default SSL certificate validation settings without implementing other security measures to compensate, (b) failed to appropriately test, audit, assess, or review its application, and (c) failed to maintain an adequate process for receiving and addressing security vulnerability comments from users.

Key Takeaways for Your Business

Subscribers to our *Privacy & Security Matters* blog are likely not surprised to see that these actions have been brought against mobile applications. As we noted back in December, an increase in enforcement actions against mobile application providers was so heavily telegraphed by the FTC and State Attorneys General in 2013 that these types of settlements were certain to follow this year. That having been said, the allegations and proposed settlement agreements highlight key lessons for online service providers and, in particular, mobile application developers going forward:

- **Understand the level of security you provide.** A key aspect to the FTC's complaints is the way in which the FTC has moved the ball forward on defining the components of "reasonable" security in the mobile sphere. The FTC describes SSL protocol as a standard security measure that is provided to application developers by iOS and Android operating systems to be applied by default. If that security measure is not implemented, then the FTC expects that compensating measures will be put in place to provide an equivalent level of protection as part of a broader comprehensive security plan.

- **Ensure proper testing and audits on an ongoing basis.** The allegations made against Fandango and Credit Karma are as much about the failure to properly test for vulnerabilities as they are about the decision to circumvent SSL in the first place. The FTC is taking the clear position that simply not knowing about security vulnerabilities is no defense for not correcting them. Audit and security procedures need to be comprehensive and effective for analyzing risks and weaknesses at all stages of the life cycle of user information, from collection to storage and disposal, and should be applied consistently on an ongoing basis. Security audit procedures should also be reviewed and updated periodically to address technological developments and new potential threats. As shown by the Credit Karma complaint, particular care should be taken to thoroughly review and assess programs and mobile applications as they move out of the testing phase.

- **Have a process specifically devoted to receiving and escalating security feedback.** Many breach incidents and security failures over the past year have been discovered by independent security researchers who have contacted organizations to inform them about the security gaps. Having a quick and effective way to receive this type of feedback can help your business get out ahead of surprises. More importantly, your users should have a fast and effective way to communicate incidents related to their accounts or information they have provided you.

- **Know what your vendors and service providers are doing.** Monitoring and auditing third-party service providers for mobile applications can be a more difficult process for mobile applications than it is for standard Web-based services. Regardless, in the Credit Karma complaint the FTC has made it clear that online service providers are ultimately responsible for knowing and understanding what kind of security processes third-party contractors are using and enforcing appropriate standards.

The proposed settlement agreements with Fandango and Credit Karma are available on the FTC's website and are open for public comment through April 28, 2014. If you have any questions about how these developments may impact your business, your Mintz Levin privacy team is here to help. You can also take advantage of resources provided by the FTC to help mobile application developers create secure applications that can be found here.

* * *

Share:

View Mintz Levin's Privacy & Security attorneys.

Read and subscribe to *Privacy & Security Matters* blog.

Boston · London · Los Angeles · New York · San Diego · San Francisco · Stamford · Washington www.mintz.com

Follow Us

Feedback: Was this mailing helpful?

This communication may be considered attorney advertising under the rules of some states. The information and materials contained herein have been provided as a service by the law firm of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.; however, the information and materials do not, and are not intended to, constitute legal advice. Neither transmission nor receipt of such information and materials will create an attorney-client relationship between the sender and receiver. The hiring of an attorney is an important decision that should not be based solely upon advertisements or solicitations. Users are advised not to take, or refrain from taking, any action based upon the information and materials contained herein without consulting legal counsel engaged for a particular matter. Furthermore, prior results do not guarantee a similar outcome.

Your e-mail address is never shared with any third parties. For more information, view our Privacy Statement.

Sign up here to receive periodic e-mails notifying you of new publications, news, and events in your areas of interest.

3846-0413-NAT-PRIV