

Mobile Enforcement Continues to be APPealing to the FTC

Alysa Z. Hutnik

April 2, 2014

On March 28, 2014, the FTC announced two new mobile app settlements – with Fandango and Credit Karma – based on allegations that the companies failed to secure the transmission of consumers’ sensitive personal information collected via their mobile apps and misrepresented the security precautions that the companies took for each app.

Specifically, the FTC alleged that Fandango and Credit Karma disabled the SSL (Secure Sockets Layer) certification validation procedure for each of their mobile apps. By doing so, the FTC claims that the apps were open to attackers positioning themselves between the app and the online service by presenting an invalid SSL certificate to the app – i.e., “man-in-the-middle” attacks. The FTC contends that Fandango and Credit Karma engaged in a number of practices that, when taken together, failed to provide reasonable and appropriate security in the development and maintenance of its mobile app, including:

- Overriding the default SSL certificate validation settings provided by the iOS and Android application programming interfaces (APIs) without implementing other security measures to compensate for the lack of SSL certificate validation;
- Failing to appropriately test, audit, assess, or review the apps, including failing to ensure that the transmission of sensitive personal information was secure;
- Failing to maintain an adequate process for receiving and addressing security vulnerability reports from third parties (*Fandango only*); and
- Failing to reasonably and appropriately oversee its service providers’ security practice (*Credit Karma only*).

The FTC also asserts that the apps made deceptive privacy and security representations, including that the deception occurred in the companies’ in-app representations.

As mobile privacy and security continues to be at the forefront of the FTC’s enforcement priorities, companies should keep abreast of developments in this area and regularly evaluate their mobile products and services. *Stay tuned for a Kelley Drye client advisory discussing the enforcement trends for mobile and “red flags” that companies should watch out for.*