Advisory

AUGUST 2017

If you have any questions about this Advisory, please contact:

JOHN KENNEDY
203-363-7640
jkennedy@wiggin.com

AARTHI ANAND
212-551-2625
aanand@wiggin.com

Uber-FTC Settlement Highlights the FTC's Focus on Aligning Security Promises with Security Practices

The Federal Trade Commission ("FTC") announced this week its settlement with Uber Technologies, Inc. ("Uber") related to certain alleged deceptive data security practices at Uber. The settlement continues the FTC's now years-long focus on alleged deceptive and unfair data security practices.

The FTC's essential allegations in its complaint were that Uber had engaged in deceptive data security and privacy practices, "[f]irst by misrepresenting the extent to which it monitored its employees' access to personal information about users and drivers, and second by misrepresenting that it took reasonable steps to secure that data."[1] As part of the settlement (or "Consent Agreement"), Uber is required to implement (a) a comprehensive privacy program, and (b) for the next twenty years, be subject to biennial third party privacy audits and maintain records and file reports confirming compliance with the Consent Agreement. The Consent Agreement includes Uber's statement that it neither admits nor denies any of the FTC's allegations in the complaint.

WHAT ATTRACTED FTC SCRUTINY

Uber's security systems were compromised in May 2014, resulting in unauthorized access of over 100,000 drivers' license information, including names and social security numbers. The breach was discovered in September 2014. At the time, Uber had publicized its privacy policy (via its website and dissemination to the press) as follows:

"Uber has a strict policy prohibiting all employees at every level from accessing a rider or driver's data. The only exception to this policy is for a limited set of legitimate business purposes. Our policy has been communicated to all employees and contractors…The policy is also clear that access to rider and driver accounts is being closely monitored and audited by data security specialists on an ongoing basis, and any violations of the policy will result in disciplinary action, including the possibility of termination and legal action."[2]

The FTC's complaint alleged that, in contrast to these security promises, Uber "has not always closely monitored and audited its employees' access to Rider and Driver accounts since November 2014." Indeed, the FTC alleged that Uber's automated system for monitoring employee access to consumer personal information in December 2014 "was not designed or staffed to effectively handle ongoing review of

CONTINUED ON NEXT PAGE

© 2017 Wiggin and Dana LLP In certain jurisdictions this may constitute attorney advertising.

Uber-FTC Settlement Highlights the FTC's Focus on Aligning Security Promises with Security Practices

access to data by Respondent's thousands of employees and contingent workers." And although Uber implemented a new automated monitoring system in August 2015, the FTC alleged that Uber still failed to monitor its employees comprehensively for potential misuse of consumer personal information, except for specific employee-generated reports about inappropriate access to co-workers.

Based on these allegations, the FTC's complaint charged that Uber's security policy was deceptive.

KEY TERMS OF THE CONSENT AGREEMENT

1. Comprehensive Privacy Program

Under the Consent Agreement, Uber is required to establish and maintain a comprehensive privacy policy that: (1) addresses "privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of Personal Information."[3] The Consent Agreement includes all of the FTC's standard injunctive measures for settlements of this kind, including:

- the designation of an employee or employees responsible for the privacy program;
- the identification of reasonably foreseeable risks, both internal and external, that could result in the unauthorized collection, use, or disclosure of Personal Information and an assessment of the sufficiency of any safeguards in place to control these risks;
- the design and implementation of reasonable controls and procedures to address such risks and regular testing or monitoring of the effectiveness of those controls and procedures;
- selecting and retaining service providers capable of protecting the privacy of Personal Information and requiring service providers, by contract, to implement and maintain privacy protections; and
- evaluation and adjustment of the privacy program in light of the results of the testing and monitoring efforts and any changes to operations that may have an impact on the effectiveness of the privacy program.

2. Third Party Audits for 20 years

Uber is also required to obtain initial and biennial assessments ("Assessments") to be completed by a "qualified, objective, independent third-party professional" approved by the FTC . After an initial report covering the first 6 months after the order, biennial reports are required for the next 20 years.

The inclusion of mandated security programs subject to a 20-year audit requirement is a standard FTC measure and has been included in most of its settlements in recent years.

CONTINUED ON NEXT PAGE

Uber-FTC Settlement Highlights the FTC's Focus on Aligning Security Promises with Security Practices

TAKEAWAYS FROM THE UBER CONSENT AGREEMENT

The FTC's settlement with Uber underscores the significance that the FTC attaches to misalignments between the security and privacy commitments made by businesses in their public disclosures in website and app privacy policies, on the one hand, and the implementation of those commitments in practice, on the other. And, as the allegations in the FTC's Uber complaint indicate, the FTC will closely scrutinize the degree to which companies abide by their privacy and security promises to consumers.

For example, the FTC investigation in this case delved not only into Uber's access control security measures with a third party (Amazon's S3 DataStore) for stored user and driver data, but also examined the company's various privacy and data security claims and statements over a two-year period. The FTC noted [4] that, during this period, communications from Uber's customer service representatives included claims such as:

- '"Your information will be stored safely and used only for purposes you've authorized. *We use the most up to date technology and services to ensure that none of these are compromised.*"
- "I understand that you do not feel comfortable sending your personal information via online. *However, we're extra vigilant in protecting all private* and personal information."
- "All of your personal information, including payment methods, *is kept secure and encrypted to the highest security standards available.*'"

Statements of this kind are frequently included in generic statements put out by companies in response to customer concerns. The FTC is now closely looking at such statements and does not confine its review of privacy claims merely to formal company disclosures such as published privacy policies.

In light of the Uber Consent Agreement and other similar FTC actions in recent years, businesses are well-advised (1) to conduct periodic reviews of how well their public privacy and security claims fit within the context of their actual privacy and security processes and third party relationships (including as these evolve over time), and (2) to be aware that the FTC's review of such claims will reach beyond the four corners of even carefully crafted privacy policies.

Footnotes:
[1] http://bit.ly/2uY81Jj

[2] See FTC's Complaint, In the Matter of Uber Technologies, Inc., paragraph 11, available at http://bit.ly/2uTVl71

CONTINUED ON NEXT PAGE

Uber-FTC Settlement Highlights the FTC's Focus on Aligning Security Promises with Security Practices

Footnotes (continued)

[3] "Personal Information" means individually identifiable information collected or received, directly or indirectly, by Respondent from or about an individual consumer, including: (a) a first and last name; (b) a physical address; (c) an email address; (d) a telephone number; (e) a Social Security number; (f) a driver's license or other government-issued identification number; (g) a financial institution account number; (h) persistent identifiers associated with a particular consumer or device; or (i) precise geo-location data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information.

[4] FTC Complaint, paragraph 17, available at http://bit.ly/2uTVl71

This publication is a summary of legal principles. Nothing in this article constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney. The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.