FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

# Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims

## Company failed to monitor access to, and provide reasonable security for, consumer data

FOR RELEASE

August 15, 2017

**TAGS:** Automobiles | Technology | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security

***Note:*** *A conference call for media with FTC Acting Chairman Maureen K. Ohlhausen and Consumer Protection Acting Director Tom Pahl will occur as follows:*

*Date: August 15, 2017*
*Time: 11 a.m. ET*
*Call-in: 800-288-8960; confirmation number 428703*

*Call-in lines, which are for* ***media only****, will open 15 minutes prior to the start of the call. FTC staff will be available to take questions from the media.*

Uber Technologies, Inc. has agreed to implement a comprehensive privacy program and obtain regular, independent audits to settle Federal Trade Commission charges that the ride-sharing company deceived consumers by failing to monitor employee access to consumer personal information and by failing to reasonably secure sensitive consumer data stored in the cloud.

In its complaint, the FTC alleged that the San Francisco-based firm failed to live up to its claims that it closely monitored employee access to consumer and driver data and that it deployed reasonable measures to secure personal information it stored on a third-party cloud provider's servers.

"Uber failed consumers in two key ways: First 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," said FTC Acting Chairman Maureen K. Ohlhausen. "This case shows that, even if you're a fast growing company, you can't leave consumers behind: you must honor your privacy and security promises."

In the wake of news reports alleging Uber employees were improperly accessing consumer data, the company issued a statement in November 2014 that it had a "strict policy prohibiting" employees from accessing rider and driver data – except for a limited set of legitimate business purposes – and that employee access would be closely monitored on an ongoing basis.

In December 2014, Uber developed an automated system for monitoring employee access to consumer personal information, but the company stopped using it less than a year after it was put in place. The FTC's complaint alleges that Uber, for more than nine months afterwards, rarely monitored internal access to personal information about users and drivers.

The FTC's complaint also alleges that despite Uber's claim that data was "securely stored within our databases," Uber's security practices failed to provide reasonable security to prevent unauthorized access to consumers' personal information in databases Uber stored with a third-party cloud provider. As a result, an intruder accessed personal information about Uber drivers in May 2014, including more than 100,000 names and driver's license numbers that Uber stored in a datastore operated by Amazon Web Services.

The FTC alleges that Uber did not take reasonable, low-cost measures that could have helped the company prevent the breach. For example, Uber did not require engineers and programmers to use distinct access keys to access personal information stored in the cloud. Instead, Uber allowed them to use a single key that gave them full administrative access to all the data, and did not require multi-factor authentication for accessing the data. In addition, Uber stored sensitive consumer information, including geolocation information, in plain readable text in database back-ups stored in the cloud.

Under its agreement with the Commission, Uber is:

- prohibited from misrepresenting how it monitors internal access to consumers' personal information;
- prohibited from misrepresenting how it protects and secures that data;
- required to implement a comprehensive privacy program that addresses privacy risks related to new and existing products and services and protects the privacy and confidentiality of personal information collected by the company; and
- required to obtain within 180 days, and every two years after that for the next 20 years, independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order.

The Commission vote to issue the administrative complaint and to accept the consent agreement was 2-0. The FTC will publish a description of the consent agreement package in the Federal Register shortly. The agreement will be subject to public comment for 30 days, beginning today and continuing through September 15, 2017, after which the Commission will decide whether to make the proposed consent order final.

Interested parties can submit comments electronically by following the instructions in the "Invitation To Comment" part of the "Supplementary Information" section.

**NOTE:** The Commission issues an administrative complaint when it has "reason to believe" that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. When the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions. Each violation of such an order may result in a civil penalty of up to $40,654.

The Federal Trade Commission works to promote competition, and protect and educate consumers. You can learn more about consumer topics and file a consumer complaint online or by calling 1-877-FTC-HELP (382-4357). Like the FTC on Facebook, follow us on Twitter, read our blogs and subscribe to press releases for the latest FTC news and resources.

# Contact Information

MEDIA CONTACT:
Nicole Jones
*Office of Public Affairs*
202-326-2565

Juliana Gruenwald Henderson
*Office of Public Affairs*
202-326-2180

STAFF CONTACTS:
Ben Rossen
*Bureau of Consumer Protection*
202-326-3679

James Trilling
*Bureau of Consumer Protection*
202-326-3497