

THE  
NATIONAL LAW REVIEW

---

## FTC Announces Expanded Settlement with Uber

---

Monday, April 16, 2018

The FTC withdrew its August 2017 administrative complaint and proposed consent agreement with Uber Technologies, Inc. (Uber) and issued a revised complaint against Uber Technologies, Inc. Uber has accepted a revised proposed consent agreement which will be subject to public comment for 30 days.

FTC's August 2017 Uber consent agreement resolved allegations that Uber had failed to live up to its claims that it closely monitored employee access to rider and driver data and that it used reasonable measures to secure personal information stored on a third-party cloud provider's servers. The previous consent agreement focused on conduct that occurred in late 2014.

Before the FTC issued the consent in final form, the FTC learned that Uber failed to disclose a significant breach of consumer data that occurred in 2016 while the FTC investigation was underway.

The revised complaint details the 2016 data breach of consumer data stored in Uber's Amazon cloud-based S3 Datastore. Specifically, it describes how intruders downloaded 16 files from the Datastore that contained unencrypted consumer personal information relating to U.S. riders and drivers. This included, among other things unencrypted personally identifying information (PII) of over 25 million names and email address, over 22 million names and mobile phone numbers, and over 600,000 names and driver's license numbers. The attackers gained access by utilizing an access key that Uber engineers used to access the S3 Datastore, which was located by the attackers in plain text in a web-based repository for computer code. According to the revised complaint, "Uber did not have a policy prohibiting engineers from reusing credentials and did not require engineers to enable multi-factor authentication" when accessing the private repositories. This allowed the attackers to use passwords that were exposed in prior data breaches to access the repositories and find the access key.

[The revised complaint](#) further describes that Uber discovered the 2016 breach after one of the attackers contacted Uber and demanded a six-figure payout. Although the attackers "maliciously exploited" the uncovered PII, Uber paid the attackers the \$100,000 through the third party that administers the company's "bug bounty" program. The program was originally created to pay financial reward in exchange for the responsible disclosure of security vulnerabilities. Uber did not disclose the breach to the FTC until November 2017, more than a year after its discovery.

The [revised consent order](#) includes a definition of "covered incident" and a new provision that requires Uber to report such incidents to the FTC along with any notice required by any federal, state, or local government entity. The requirement to report breaches to the FTC is similar to the HIPAA statutory scheme that requires that certain breaches be reported to HHS's Office of Civil Rights.

The revised order is broadened to require that Uber submit all the reports from the required third-party audits of Uber's privacy program rather than only the initial report to the FTC. Finally, certain of the recordkeeping requirements have been extended from three to five years and must also provide all copies of subpoenas and other communications with law enforcement related to compliance with the order and all records which call into question Uber's compliance with the order.

It is very unusual for the FTC to take the action it has taken with Uber. Had the ink been dry and the order final, it is possible that the facts surrounding the 2016 breach would have been found to violate the order. If the FTC had determined that the order was violated, it would be able to seek civil penalties. Instead, the FTC broadened the complaint allegations and the order. It should be noted that the commission has requested that U.S. Congress



Article By [Anand Raj Shah](#)  
[Katherine E. Armstrong](#)  
[Drinker Biddle & Reath LLPDBR on Data](#)

[Communications, Media & Internet](#)  
[Litigation / Trial Practice](#)  
[All Federal](#)

grant it civil penalty authority for data security breaches.

© 2019 Drinker Biddle & Reath LLP. All Rights Reserved

**Source URL:** <https://www.natlawreview.com/article/ftc-announces-expanded-settlement-uber>