Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Uber Technologies, Inc., File No. 1523054

The Federal Trade Commission has withdrawn its acceptance of the agreement containing consent order from Uber Technologies, Inc. ("Uber") that the Commission released for public comment in this proceeding on August 15, 2017 ("August 2017 proposed consent agreement"), and has accepted, subject to final approval, a new agreement containing consent order from Uber ("April 2018 proposed consent agreement").

The April 2018 proposed consent agreement has been placed on the public record for thirty (30) days for receipt of comments by interested persons. All comments received during this period will become part of the public record. Interested persons who submitted comments during the public comment period for the August 2017 proposed consent agreement should resubmit their original comments, or submit new comments, during the new comment period if they would like the Commission to consider their comments when the Commission decides whether to make final the April 2018 proposed consent agreement. After thirty (30) days, the Commission again will review the April 2018 proposed consent agreement, and the comments received, and will decide whether it should withdraw from the agreement or make final the agreement's proposed order.

Since 2010, Uber has operated a mobile application (the "App") that connects consumers who are transportation providers ("Drivers") with consumers seeking those services ("Riders"). Riders book transportation or delivery services through a publicly-available version of the App that can be downloaded A postal addresses, Social Security numbers, driver's license numbers, bank a vehicle registration information, and insurance information. With respect to Riders, Uber collects names, email addresses, postal addresses, and detailed trip records with precise geolocation information, among other things.

In November 2014, Uber was the subject of various news reports describing improper access and use of consumer personal information, including geolocation information, by Uber employees. One article reported that an Uber executive had suggested that Uber should hire "opposition researchers" to look into the "personal lives" of journalists who criticized Uber's practices. Another article described an aerial tracking tool known as "God View" that displayed the personal information of Riders using Uber's services. These reports led to considerable consumer uproar. In an effort to respond to consumer concerns, Uber issued a statement describing its policies concerning access to Rider and Driver data. As part of that statement, Uber promised that all "access to rider and driver accounts is being closely monitored and

As described below, count two of the proposed complaint alleges that the above statements violated Section 5 of the FTC Act because Uber engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to Rider and Driver personal information in the Amazon S3 Datastore.[2] Specifically, Uber allegedly:

- Failed to implement reasonable access controls to safeguard data stored in the Amazon S3 Datastore. For example, Uber (1) until approximately September 2014, permitted engineers to access the Amazon S3 Datastore with a single, shared AWS access key that provided full administrative privileges over all data stored there; (2) until approximately September 2014, failed to restrict access to systems based on employees' job functions; and (3) until approximately September 2015, failed to require multi-factor authentication for individual account access, and until at least November 2016, failed to require multi-factor authentication for programmatic service account access, to the Amazon S3 Datastore;

- Until at least September 2014, failed to implement reasonable security training and guidance;

- Until approximately September 2014, failed to have a written information security program; and

- Until at least November 2016, stored sensitive personal information in the Amazon S3 Datastore in clear, readable text, rather than encrypting the information.

As a result of these failures, intruders accessed Uber's Amazon S3 Datastore multiple times using access keys that Uber engineers had posted to GitHub, a code-sharing site used by software developers.

First, on or about May 12, 2014, an intruder accessed Uber's Amazon S3 Datastore using an access key that was publicly posted and granted full administrative privileges to all data and documents stored within Uber's Amazon S3 Datastore (the "2014 data breach"). The intruder accessed one file that contained sensitive personal information belonging to Uber Drivers, including over 100,000 unencrypted names and driver's license numbers, 215 unencrypted names and bank account and domestic routing numbers, and 84 unencrypted names and Social Security numbers. Uber did not discover the breach until September 2014. Uber sent breach

notification letters to affected Uber Drivers in February 2015. Uber later learned of more affected Uber Drivers in May and July 2016 and sent breach notification letters to those Drivers in June and August 2016.

Second, between October 13, 2016 and November 15, 2016, intruders accessed Uber's Amazon S3 Datastore using an AWS access key that was posted to a private GitHub repository ("the 2016 data breach"). Uber granted its engineers access to Uber's GitHub repositories through engineers' individual GitHub accounts, which engineers generally accessed through personal email addresses. Uber did not have a policy prohibiting engineers from reusing credentials, and did not require engineers to enable two-factor authentication when accessing Uber's GitHub repositories. The intruders who committed the 2016 breach said that they accessed Uber's GitHub page using passwords that were previously exposed in other large data breaches, whereupon they discovered the AWS access key they used to access and download files from Uber's Amazon S3 Datastore. The intruders downloaded approximately 25.6 million unique email addresses, 22.1 millio

The purpose of this analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify in any way the proposed order's terms.