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The Federal Trade Commission has withdrawn its acceptance of the agreement containing consent order from Uber Technologies, Inc. ("Uber") that the Commission released for public comment in this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 to a smartphone. When a Rider requests transportation through the App, the request is conveyed to a nearby Uber Driver signed into the App.

Drivers use the App to determine which ride requests they will accept. Uber collects a variety of personal information from Drivers, including names, email addresses, phone numbers, postal addresses, Social Security numbers, driver's license numbers, bank account information, 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

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."

As alleged in the proposed complaint, Uber has not monitored or audited its employees' access to Rider and Driver personal information on an ongoing basis since November 2014. In fact, between approximately August 2015 and May 2016, Uber did not timely follow up on automated alerts concerning the potential misuse of consumer personal information, and for approximately the first six months of this period only monitored access to account information belonging to a set of internal high-profile users, such as Uber executives. During this time, Uber did not otherwise monitor internal access to personal information unless an employee specifically reported that a co-worker had engaged in improper access. Count one of the proposed complaint alleges that Uber's representation that it closely monitored and audited internal access to consumers' personal information was false or misleading in violation of Section 5 of the FTC Act in light of Uber's subsequent failure to monitor and audit such access between August 2015 and May 2016.[1]

The proposed complaint also alleges that Uber failed to provide reasonable security for consumer information stored in a third-party cloud storage service provided by Amazon Web Services ("AWS") called the Amazon Simple Storage Service (the "Amazon S3 Datastore"). Uber stores in the Amazon S3 Datastore a variety of files that contain sensitive personal information, including full and partial back-ups of Uber databases. These back-ups contain a broad range of Rider and Driver personal information, including, among other things, names, email addresses, phone numbers, driver's license numbers, and trip records with precise geolocation information.

From July 13, 2013 to July 15, 2015, Uber's privacy policy described the security measures Uber used to protect the personal information it collected from consumers, stating that such information "is securely stored within our databases, and we use standard, industry-wide commercially reasonable security practices such as encryption, firewalls and SSL (Secure Socket Layers) for protecting your information—such as any portions of your credit card number which we retain… and geo-location information." Additionally, Uber's customer service representatives offered assurances about the strength of Uber's security practices to consumers who were reluctant to submit personal information to Uber.

[1] Count one of the proposed complaint and the underlying factual allegations are unchanged from the proposed complaint against Uber that the Commission issued previously as part of the August 2017 proposed consent agreement.

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

[2] Count two of the proposed complaint addresses the same allegedly false or misleading statements as did count two of the proposed complaint against Uber that the Commission issued as part of the August 2017 proposed consent agreement. The proposed complaint includes allegations that the now withdrawn complaint included to support count two and also includes additional allegations to support count two based on new information the Commission obtained after August 2017.

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 multi-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 sixteen files that contained unencrypted consumer personal information relating to U.S. Riders and Drivers, including approximately 25.6 million names and email addresses, 22.1 million names and mobile phone numbers, and 607,000 names and driver's license numbers. Nearly all of the exposed personal information was collected before July 2015 and stored in unencrypted database backup files.

Uber discovered the 2016 data breach on or about November 14, 2016, when one of the attackers contacted Uber claiming to have compromised Uber's "databases" and demanding a six-figure payout. Uber paid the attackers $100,000 through the third party that administers Uber's "bug bounty" program. Respondent created the bug bounty program to pay financial rewards in exchange for the responsible disclosure of serious security vulnerabilities. However, the attackers who committed the 2016 data breach were fundamentally different from legitimate bug bounty recipients. Instead of responsibly disclosing a vulnerability, the attackers maliciously exploited the vulnerability and acquired millions of consumers' personal information.

Uber failed to disclose the 2016 data breach to affected consumers until November 21, 2017, more than a year after discovering it. Uber also failed to disclose the 2016 data breach to the Commission until November 2017 despite the fact that the breach occurred in the midst of a nonpublic Commission investigation relating to Uber's data security practices, including, specifically, the security of Uber's Amazon S3 Datastore.

The proposed consent order contains provisions designed to prevent Uber from engaging in acts and practices in the future similar to those alleged in the proposed complaint.

Part I of the proposed order prohibits Uber from making any misrepresentations about the extent to which Uber monitors or audits internal access to consumers' personal information or the extent to which Uber protects the privacy, confidentiality, security, or integrity of consumers' personal information. This Part is identical to Part I of the August 2017 proposed consent agreement.

Part II of the proposed order requires Uber to implement a mandated comprehensive privacy program that is reasonably designed to (1) address 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 consumers' personal information. Part II.B includes new language that requires Uber's mandated privacy risk assessments to include consideration of risks and safeguards related to (a) secure software design, development, and testing, including access key and secret key management and secure cloud storage; (b) review, assessment, and response to third-party security vulnerability reports, including through a "bug bounty" or similar program; and (c) prevention, detection, and response to attacks, intrusions, or systems failures.

Part III of the proposed order requires Uber to undergo biennial assessments of its mandated privacy program by a third party. Part III has been revised from the August 2017 proposed consent agreement to require Uber to submit to the Commission each of its assessments rather than only its initial assessment.

Part IV of the proposed order requires Uber to submit a report to the Commission if Uber discovers any "covered incident" involving unauthorized access or acquisition of consumer information. This Part is new.

Parts V through IX of the proposed order are reporting and compliance provisions. Part V requires dissemination of the order now and in the future to all current and future principals, officers, directors, and managers, and to persons who participate in conduct related to the subject matter of the order, including all employees, agents, and representatives who regularly access personal information. Part VI mandates that Uber submit a compliance report to the FTC one year after issuance of the order and submit additional notices as specified. Parts VII and VIII require Uber to retain documents relating to its compliance with the order, and to provide such additional information or documents as are necessary for the Commission to monitor compliance. Part IX states that the order will remain in effect for 20 years.

These provisions include modifications from the August 2017 proposed consent agreement. Part V expands the acknowledgement of order provision to require Uber to obtain signed acknowledgements from all employees, agents, and representatives who regularly access personal information that Uber collects or receives from or about consumers, rather than limiting the requirement to employees with managerial responsibility related to the order. And Part VII contains modified recordkeeping provisions and new recordkeeping provisions relating to Uber's bug bounty program and its subpoenas and communications with law enforcement.

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.