This document is scheduled to be published in the
Federal Register on 08/21/2017 and available online at
https://federalregister.gov/d/2017-17526, and on **FDsys.gov**

[BILLING CODE: 6750-01S]

FEDERAL TRADE COMMISSION

[File No. 152 3054]

Uber Technologies, Inc.; Analysis to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed Consent Agreement.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis to Aid Public Comment describes both the allegations in the complaint and the terms of the consent order -- embodied in the consent agreement -- that would settle these allegations.

DATES: Comments must be received on or before September 15, 2017.

ADDRESSES: Interested parties may file a comment online or on paper, by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write: "In the Matter of Uber Technologies, Inc., File No. 152-3054" on your comment, and file your comment online at https://ftcpublic.commentworks.com/ftc/ubertechconsent by following the instructions on the web-based form. If you prefer to file your comment on paper, write "In the Matter of Uber Technologies, Inc., File No. 152-3054" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue, NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street, SW, 5th Floor, Suite 5610 (Annex D), Washington, DC

20024.

FOR FURTHER INFORMATION CONTACT: Ben Rossen (202-326-3679) and James Trilling (202-326-3497), Bureau of Consumer Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR § 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement, and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained from the FTC Home Page (for August 15, 2017), on the World Wide Web, at https://www.ftc.gov/news-events/commission-actions.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before September 15, 2017. Write "In the Matter of Uber Technologies, Inc., File No. 152-3054" on your comment. Your comment - including your name and your state - will be placed on the public record of this proceeding, including, to the extent practicable, on the public Commission Website, at https://www.ftc.gov/policy/public-comments.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online. To make sure that the Commission considers your online comment, you must file it at https://ftcpublic.commentworks.com/ftc/ubertechconsent by following the instructions on the

web-based form. If this Notice appears at http://www.regulations.gov/#!home, you also may file a comment through that website.

If you prefer to file your comment on paper, write "In the Matter of Uber Technologies, Inc., File No. 152-3054" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue, NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street, SW, 5th Floor, Suite 5610 (Annex D), Washington, DC. 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible FTC Website at https://www.ftc.gov, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential" – as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2) – including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the public FTC Website – as legally required by FTC Rule 4.9(b) – we cannot redact or remove your comment from the FTC Website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at http://www.ftc.gov to read this Notice and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before September 15, 2017. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see https://www.ftc.gov/site-information/privacy-policy.

Analysis of Agreement Containing Consent Order to Aid Public Comment

The Federal Trade Commission has accepted, subject to final approval, an agreement containing a consent order from Uber Technologies, Inc. ("Uber").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission again will review the

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 are consumers who 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 and calls by consumers to stop using Uber's services. 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. 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.

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 a variety of files in the Amazon S3 Datastore 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.

As described below, 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. Specifically, Uber allegedly:

- Until approximately September 2014, failed to implement reasonable access controls to safeguard data stored in the Amazon S3 Datastore. For example, Uber (1) 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) failed to restrict access to systems based on employees' job functions; and (3) failed to require multi-factor authentication for access to the Amazon S3 Datastore;
- Until approximately September 2014, failed to implement reasonable security training and guidance;
- Until approximately September 2014, failed to have a written information security program; and

- Until approximately March 2015, stored sensitive personal information in the Amazon S3 Datastore in clear, readable text, rather than encrypting the information.

As a result of these failures, on or about May 12, 2014, an intruder was able to gain access to Uber's Amazon S3 Datastore using an access key that one of Uber's engineers had posted to GitHub, a code-sharing site used by software developers. This key was publicly posted and granted full administrative privileges to all data and documents stored within Uber's Amazon S3 Datastore. 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, at which time Uber took steps to prevent further unauthorized access.

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

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.

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 III of the proposed order requires Uber to undergo biennial assessments of its mandated privacy program by a third party.

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

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.

By direction of the Commission.

Donald S. Clark,
Secretary.

[FR Doc. 2017-17526 Filed: 8/18/2017 8:45 am; Publication Date: 8/21/2017]