1523054

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Joseph J. Simons, Chairman
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of	)	
	)	DOCKET NO. C-4662
Uber Technologies, Inc., a corporation.	)	

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that Uber Technologies, Inc. ("Respondent" or "Uber"), a corporation, has violated the Federal Trade Commission Act, 15 U.S.C. § 45(a), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Uber is a Delaware corporation with its principal office or place of business at 1455 Market St. #400, San Francisco, California 94103.

2. The acts and practices of Respondent alleged in this Complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS PRACTICES

3. Since at least 2010, Respondent has distributed a mobile software application (the "App") that connects consumers who are transportation providers (hereinafter "Uber Drivers" or "Drivers") with consumers seeking those services (hereinafter "Riders"). Respondent markets different versions of the App to Riders and Drivers. Respondent also operates a website at www.uber.com.

4. Riders book transportation services from an Uber Driver using 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.

5. Uber Drivers are consumers who use the App to locate Riders in need of transportation. Respondent recruits and approves consumers to become Uber Drivers, sets the rates that Drivers charge for providing transportation, and collects a portion of the fares that Drivers

charge for each ride. Drivers decide when they are available to accept ride requests and use the App to determine which ride requests they will accept.

6. When a consumer signs up to become an Uber Driver, Respondent collects personal

> The policy is also clear that 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.

(Exhibit A.)

12. Despite Respondent's representation that its practices would continue on an ongoing basis, Respondent has not always closely monitored and audited its employees' access to Rider and Driver accounts since November 2014. Respondent developed an automated system for monitoring employee access to consumer personal information in December 2014 but the system was not designed or staffed to effectively handle ongoing review of access to data by Respondent's thousands of employees and contingent workers.

13. In approximately August 2015, Respondent ceased using the automated system it had developed in December 2014 and began to develop a new automated monitoring system. From approximately August 1st, 2015 until May 12, 2016, Respondent

The Personal Information and Usage Information we collect is securely stored within our databases, and we use standard, industry-

2016, failed to require multi-factor authentication for programmatic service account access to the Amazon S3 Datastore;

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

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

d. Until at least November 2016, stored sensitive personal information in the Amazon S3 Datastore in clear, readable text, including in database backup and database prune files, rather than encrypting the information.

19. Respondent could have prevented or mitigated the failures described in Paragraph 18 through relatively low-cost measures.

20. Respondent's failure to provide reasonable security for consumers' personal information stored in its databases, including geolocation information, created serious risks for consumers.

2014 DATA BREACH

21. As a result of the failures described in Paragraph 18, on or about May 12, 2014, an intruder was able to access consumers' personal information in plain text in Respondent's Amazon S3 Datastore using an access key that one of Respondent's engineers had publicly posted to GitHub, a code-sharing website used by software developers. The publicly posted key granted full administrative privileges to all data and documents stored within Respondent'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. The file also contained other Uber Driver information, including physical addresses, email addresses, mobile device phone numbers, device IDs, and location information from trips the Uber Drivers provided.

22. Respondent did not discover the existence of the breach until September 2014.

23. Respondent initially sent breach notification letters to 48,949 affected Uber Drivers in February 2015. In May and July of 2016, Uber learned of more individuals affected by the breach, including approximately 60,000 additional Uber Drivers whose unencrypted names and driver's license numbers were accessed. Uber sent additional breach notification letters to these affected Uber Drivers in June and August of 2016.

2016 DATA BREACH

24. On or about November 14, 2016, Respondent learned of another breach of consumer personal information stored in Uber's Amazon S3 Datastore. Once again, intruders gained access to the Amazon S3 Datastore using an access key that an Uber engineer had posted to GitHub. This time, the key was in plain text in code that was posted to a private GitHub

COUNT 2

30. As described in Paragraphs 16 -17, Respondent has represented, directly or indirectly, expressly or by implication, that it would provide reasonable security for consumers' personal information stored in its databases.

31. In truth and in fact, as described in Paragraphs 18 -27, Respondent did not provide reasonable security for consumers' personal information stored in its databases. Therefore, the representation set forth in Paragraph 30 is false or misleading.

32. The acts and practices of Respondent as alleged in this Complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this twenty-fifth day of October, 2018, has issued this Complaint against Respondent.

By the Commission, Commissioner Wilson not participating.

Donald S. Clark
Secretary

SEAL: