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 information about the consumer, including the consumer's name, email address, phone number, postal address, profile picture, Social Security number, driver's license information, bank account information (including domestic routing and bank account numbers), vehicle registration information, and insurance information.

7. Respondent also collects and stores a variety of personal information from Riders, including, among other things, names, email addresses, postal addresses, profile pictures, and detailed trip records including precise geolocation information.

8. Respondent collects precise geolocation information about both Riders and Drivers in real time. When a Rider requests transportation services and has authorized Respondent to collect such information, Respondent collects precise geolocation information from the Rider's device. During a trip, Respondent collects precise geolocation information from the Rider's device if the Rider has provided consent for Respondent to do so. Respondent also collects such information about the route of the trip from the Driver's mobile device and associates the trip information with the Rider.

9. As of December 2014, there were more than 160,000 active Uber Drivers using the App. As of December 2015, Riders had completed more than 1 billion rides using Respondent's services. In 2015, Respondent had over $1.5 billion in total revenues.

RESPONDENT'S INTERNAL ACCESS TO CONSUMER PERSONAL INFORMATION

10. In November 2014, Respondent was the subject of a number of widely disseminated news reports concerning allegations of improper access and use of consumer personal information, including geolocation data. One article, published on November 17, 2014, reported that an Uber executive had suggested Respondent should hire "opposition researchers" and journalists to look into the "personal lives" of journalists who criticized Respondent's business practices. On November 18, 2014, another article described an internal aerial tracking tool, referred to as "God View," that displayed the personal information of Riders using Respondent's services. These reports were widely circulated in the press and caused considerable consumer uproar.

11. In an effort to respond to consumer concerns, on November 18, 2014, Respondent issued a statement, which has been continuously posted on Respondent's website and was widely disseminated in the press, describing Respondent's policies concerning access to Rider and Driver data. Respondent stated:

> Uber has a strict policy prohibiting all employees at every level from accessing a rider or driver's data. The only exception to this policy is for a limited set of legitimate business purposes. Our policy has been communicated to all employees and contractors….

> 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 2015 until May 2016, Respondent 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, Respondent only monitored access to account information belonging to a set of internal high-profile users, such as Uber executives. During this time, Respondent did not otherwise monitor internal access to personal information unless an employee specifically reported that a co-worker had engaged in inappropriate access.

RESPONDENT'S AMAZON S3 DATASTORE

14. As part of its information technology infrastructure, Respondent uses a third-party service provided by Amazon Web Services ("AWS") called the Amazon Simple Storage Service (the "Amazon S3 Datastore"). The Amazon S3 Datastore is a scalable cloud storage service that can be used to store and retrieve large amounts of data. The Amazon S3 Datastore stores data inside of virtual containers, called "buckets," against which individual access controls can be applied.

15. Respondent relies on the Amazon S3 Datastore to store a wide variety of files that contain sensitive personal information. These files include, among other things, full and partial back-ups of Uber databases. The database back-ups contain a broad range of Rider and Driver personal information, including, among other things, names, nicknames, email addresses, postal addresses, phone numbers, unique device identifiers, trip records, geolocation information, and driver's license numbers. The files also include documents provided by Uber Drivers, such as vehicle registration receipts, proof of insurance documents, and images of driver's licenses.

RESPONDENT'S SECURITY STATEMENTS

16. From at least July 13, 2013 to July 15, 2015, Respondent disseminated, or caused to be disseminated, a privacy policy that expressly applied to Respondent's websites and Apps and contained the following statements regarding the security measures Respondent used to protect the personal information it collected from consumers:

> The Personal Information and Usage Information we collect 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 (we do not ourselves retain your entire credit card information) and geo-location information.

(Exhibit B.)

17. In numerous instances, Respondent's customer service representatives offered assurances about the strength of Respondent's security practices to consumers who were reluctant to submit personal information to Uber, including but not limited to the following:

> "Your information will be stored safely and used only for purposes you've authorized. **We use the most up to date technology and services to ensure that none of these are compromised**."
>
> "I understand that you do not feel comfortable sending your personal information via online. However, **we're extra vigilant in protecting all private and personal information**."
>
> "All of your personal information, including payment methods, is **kept secure and encrypted to the highest security standards available**."

(Emphases added.)

RESPONDENT'S SECURITY PRACTICES

18. Respondent has engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to Rider and Driver personal information stored in the Amazon S3 Datastore. Among other things, Respondent:

    a. Failed to implement reasonable access controls to safeguard data stored in the Amazon S3 Datastore. For example, Respondent:

        i. until approximately September 2014, failed to require programs and engineers that access the Amazon S3 Datastore to use distinct access keys, instead permitting all programs and engineers to use a single AWS access key that provided full administrative privileges over all data in the Amazon S3 Datastore;

        ii. until approximately September 2014, failed to restrict access to systems based on employees' job functions; and

        iii. 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;

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 back-ups 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

repository. However, 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 said that they accessed Uber's GitHub page using passwords that were previously exposed in other large data breaches, whereupon they discovered the access key in plain text. The intruders downloaded 16 files from Respondent's Amazon S3 Datastore between October 13, 2016 and November 15, 2016. These files contained unencrypted consumer personal information relating to U.S. Riders and Drivers, including, among other things, 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.

25. Respondent discovered the breach on or about November 14, 2016, when one of the attackers contacted Respondent claiming to have compromised Uber's "databases" and demanding a six-figure payout.

26. Respondent 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 in this instance were fundamentally different from legitimate bug bounty recipients. These attackers did not merely identify a vulnerability and disclose it responsibly. Rather, the attackers maliciously exploited the vulnerability and acquired personal information relating to millions of consumers.

27. Respondent failed to disclose the breach to affected consumers until November 21, 2017, more than a year after discovery of the breach. Furthermore, the November 2016 breach occurred in the midst of a nonpublic investigation by the Commission relating to Respondent's data security practices, including, specifically, the security of Respondent's Amazon S3 Datastore. Despite the pendency of this investigation, Respondent failed to disclose the existence of the breach to the Commission until November 2017.

COUNT 1

28. As described in **Paragraph 11**, Respondent has represented, directly or indirectly, expressly or by implication, that internal access to consumers' personal information is closely monitored and audited by data security specialists on an ongoing basis.

29. In truth and in fact, as described in **Paragraphs 12 - 13**, Respondent has not closely monitored and audited internal access to consumers' personal information by data security specialists on an ongoing basis. Therefore, the representation set forth in **Paragraph 28** is false or misleading.

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: