1523054

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Maureen K. Ohlhausen, Acting Chairman
Terrell McSweeny

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

COMP

Commission Act, 15 U.S.C. § 45(a), and it appearing to the Comm
in the public interest, alleges:

1. Respondent Uber is a Delaware corporation with its principal
1455 Market St. #400, San Francisco, California 94103.

2. The acts and practices of Respondent alleged in this Complaint hav
commerce, as "commerce" is defined in Section 4 of the Fede

RESPONDENT'S BUSINESS PRACTICE

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

4. Riders book transportation services from an Uber Driver using a pu
the App that can be downloaded to a smartphone. When a Rider re
through the App, the request is conveyed to a nearby Uber Driver si

5. Uber Drivers are consumers who use the App to locate Riders in ne
Respondent recruits and approves consumers to become Uber Drive
Drivers charge for providing transportation, and collects a portion o
charge for each ride. Drivers decide when they are available to acc
the App to determine which ride requests they will accept.

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

(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 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 Datad-26(y)19 0 ad-26(y

any portions of your credit card number which we retain (we do not ourselves retain your entire credit card information) and 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

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 _____ day of _____, 2018, has issued this Complaint against Respondent.

By the Commission.

Donald S. Clark
Secretary

SEAL: