SUPERIOR COURT OF THE DISTRICT OF COLUMBIA
Civil Division

DISTRICT OF COLUMBIA,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Civil Action No. 18-____
	)	
UBER TECHNOLOGIES, INC.	)	
	)	
Defendant.	)	

FINAL JUDGMENT AND CONSENT DECREE

Plaintiff District of Columbia ("District"), by and through the Attorney General, has filed a Complaint for a permanent injunction and other relief in this matter pursuant to D.C. Code §§ 28-3909 and 28–3853, alleging Defendant, UBER TECHNOLOGIES, INC. ("UBER"), committed violations of the Consumer Protection Procedures Act ("CPPA"), D.C. Code §§ 28-3901, *et seq.* and the Consumer Security Breach Notification Act ("CSBNA"), D.C. Code §§ 28-3851, *et seq.*

Plaintiff and UBER have agreed to the Court's entry of this Final Judgment and Consent Decree without trial or adjudication of any issue of fact or law, and without admission of any facts alleged or liability of any kind.

Preamble

The Attorneys General of the states and commonwealths of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii[1], Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland[2], Massachusetts,

[1] Hawaii is represented by its Office of Consumer Protection. For simplicity purposes, the entire group will be referred to as the "Attorneys General," or individually as "Attorney General." Such designations, however, as they pertain to Hawaii, shall refer to the Executive Director of the State of Hawaii Office of Consumer Protection.
[2] The use of the designations "Attorneys General" or "Attorney General," as they pertain to Maryland, shall refer to the Consumer Protection Division of the Office of the Maryland Attorney General.

Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah[3], Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming, and the District of Columbia (collectively, the "Attorneys General," or the "States") conducted an investigation under their respective State Consumer Protection Acts and Personal Information Protection Acts[4] regarding the data breach involving UBER that occurred in 2016 and that UBER announced in 2017.

Parties

1. The Attorney General is authorized to enforce the District's consumer protection laws, including the CPPA and CSBNA.
2. UBER is a Delaware corporation with its principal place of business at 1455 Market Street, San Francisco, California 94103.
3. As used herein, any reference to "UBER" or "Defendant" shall mean UBER TECHNOLOGIES, INC., including all of its officers, directors, affiliates, subsidiaries and divisions, predecessors, successors and assigns doing business in the United States. However, any affiliate or subsidiary created as a result of an acquisition by UBER after the Effective Date shall not be subject to any requirement of this Final Judgment and Consent Decree until ninety (90) days after the acquisition closes.

[3] Claims pursuant to the Utah Protection of Personal Information Act are brought under the direct enforcement authority of the Attorney General. Utah Code § 13-44-301(1). Claims pursuant to the Utah Consumer Sales Practices Act are brought by the Attorney General as counsel for the Utah Division of Consumer Protection, pursuant to the Division's enforcement authority. Utah Code §§ 13-2-1 and 6.

[4] State law citations (UDAP and PIPAs) – *See Appendix A.*

Findings

4. The Court has jurisdiction over the subject matter of the complaint filed herein and over the parties to this Final Judgment and Consent Decree.
5. At all times relevant to this matter, UBER engaged in trade and commerce affecting consumers in the States, including in Washington, D.C. ("D.C."), in that UBER is a technology company that provides a ride hailing mobile application that connects drivers with riders. Riders hail and pay drivers using the UBER platform.

Order

NOW THEREFORE, on the basis of these findings, and for the purpose of effecting this Final Judgment and Consent Decree, IT IS HEREBY ORDERED AS FOLLOWS:

I. DEFINITIONS

1. "Covered Conduct" shall mean UBER's conduct related to the data breach involving UBER that occurred in 2016 and that UBER announced in 2017.
2. "Data Security Incident" shall mean any unauthorized access to Personal Information owned, licensed, or maintained by UBER.
3. "Effective Date" shall be October 25, 2018.
4. "Encrypt," "Encrypted," or "Encryption" shall mean rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.
5. "Personal Information" shall have the definition as set forth in the CSBNA, D.C. Code § 28–3851.
6. "Riders and Drivers" or, as applicable, "Rider or Driver" shall mean any individual natural person who is a resident of D.C. who uses UBER's ride hailing mobile applications to request or receive transportation (i.e., riders) or to provide transportation

individually or through partner transportation companies (i.e., drivers), other than in connection with Uber Freight or similar services offered by UBER to commercial enterprises.

7. "Security Executive" shall be an executive or officer with appropriate background and experience in information security who is designated by UBER as responsible for the Information Security Program. The title of such individual need not be Security Executive.

II. INJUNCTIVE RELIEF

8. The injunctive terms contained in this Final Judgment and Consent Decree are being entered pursuant to D.C. Code § 28–3909. Uber shall implement and thereafter maintain the practices described below, including continuing those of the practices that it has already implemented.
9. UBER shall comply with the CPPA and the CSBNA in connection with its collection, maintenance, and safeguarding of Personal Information.
10. UBER shall not misrepresent the extent to which UBER maintains and/or protects the privacy, security, confidentiality, or integrity of any Personal Information collected from or about Riders and Drivers.
11. UBER shall comply with the reporting and notification requirements of the CSBNA.
12. Specific Data Security Safeguards. No later than ninety (90) days after the Effective Date and for a period of ten (10) years thereafter, UBER shall:
    a. Prohibit the use of any cloud-based service or platform from a third party for developing or collaborating on code containing any plaintext credential if that credential provides access to a system, service, or location that contains Personal Information of a Rider or Driver unless:

i. UBER has taken reasonable steps to evaluate the data security measures and access controls provided by the service or platform as implemented by UBER;

ii. UBER has determined that the data security measures and access controls are reasonable and appropriate in light of the sensitivity of the Personal Information that a plaintext credential appearing in code on the service or platform can access;

iii. UBER has documented its determination in writing; and

iv. UBER's Security Executive or her or his designee has approved the use of the service or platform.

Access controls for such service or platform shall not be considered reasonable and appropriate if they do not include password protection including strong, unique password requirements and multifactor authentication, *or* the equivalent level of protection through other means such as single sign-on; appropriate account lockout thresholds; and access logs maintained for an appropriate period of time.

b. Maintain a password policy for all employees that includes strong password requirements.

c. Develop, implement, and maintain a policy regarding the Encryption of Personal Information of Riders and Drivers in the following circumstances. First, the policy shall require the use of Encryption when such information is transmitted electronically over a network. Second, the policy shall require the use of Encryption for backups of databases containing such information when the backups are stored on a third-party, cloud-based service or platform, either

through Encryption of Personal Information of Riders and Drivers within the backup or through Encryption of the backup file or location where it is stored. To the extent UBER determines that such Encryption is not reasonably feasible in a particular instance, UBER may instead use effective alternative compensating controls reviewed and approved by UBER's Security Executive or her or his designee.

13. Information Security Program

a. Within one hundred twenty (120) days after the Effective Date, UBER shall develop, implement, and maintain a comprehensive information security program ("Information Security Program") reasonably designed to protect the security, integrity, and confidentiality of Personal Information collected from or about Riders and Drivers.

b. The Information Security Program shall be at least compliant with any applicable requirements under District law, and at a minimum, shall be written and shall contain administrative, technical, and physical safeguards appropriate to:

    i. The size and complexity of UBER's operations;

    ii. The nature and scope of UBER's activities; and

    iii. The sensitivity of the Personal Information of Riders and Drivers that UBER maintains.

c. At a minimum, the Information Security Program shall include:

    i. regular identification of internal and external risks to the security, confidentiality, or integrity of Personal Information of Riders and Drivers that could result in the unauthorized disclosure, misuse, loss, alteration,

destruction, or other compromise of such information, and an assessment of the sufficiency of any safeguards in place to control these risks;

ii. the design and implementation of reasonable safeguards to control these risks;

iii. regular testing and monitoring of the effectiveness of these safeguards;

iv. the evaluation and adjustment of the Information Security Program in light of the results of the testing and monitoring; and

v. ongoing training of employees and temporary, contract, and contingent workers concerning the proper handling and protection of Personal Information of Riders and Drivers, the safeguarding of passwords and security credentials for the purpose of preventing unauthorized access to Personal Information, and disciplinary measures for violation of the Information Security Program, including up to termination for employees and permanent removal from UBER for temporary, contract, and contingent workers.

d. UBER shall ensure that its Information Security Program receives the resources and support reasonably necessary to ensure that the Information Security Program functions as intended.

e. UBER shall designate a Security Executive who shall be responsible for the Information Security Program.

14. Information Security Program Assessments

a. Within one year of the Effective Date and biennially for ten (10) years thereafter, UBER shall obtain assessments of its Information Security Program.

b. The assessments shall be performed by an independent third party that: (a) is a Certified Information Systems Security Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or a similarly qualified person or organization; and (b) has at least five (5) years of experience evaluating the effectiveness of computer systems or information system security.

c. The assessments shall set forth the administrative, technical, and physical safeguards maintained by UBER and explain the extent to which the safeguards are appropriate to UBER's size and complexity, the nature and scope of UBER's activities, and the sensitivity of Personal Information of Riders and Drivers that UBER maintains, and thereby meet the requirements of the Information Security Program.

d. UBER shall provide a copy of the third party's final written report of each assessment to the California Attorney General's Office within one hundred twenty (120) days after the assessment has been completed.

    i. Confidentiality: The California Attorney General's Office shall treat the report as exempt from disclosure under the relevant public records laws.

    ii. State Access: The California Attorney General's Office may provide a copy of the report received from UBER to any other of the Attorneys General upon request, and each requesting Attorney General shall treat such report as exempt from disclosure as applicable under the relevant public records laws.

15. Incident Response and Data Breach Notification Plan

a. For a period of two (2) years following the Effective Date, UBER shall report on at least a quarterly basis to the District identifying and describing any Data

Security Incidents that occurred during the reporting period and are required by any U.S. federal, state, or local law or regulation to be reported to any U.S. federal, state, or local government entity.

b. UBER shall maintain a comprehensive Incident Response and Data Breach Notification Plan ("Plan"). At a minimum, the Plan shall:

   i. identify the types of incidents that fall within the scope of the Plan, which must include any incident that UBER reasonably believes might be a Data Security Incident;

   ii. clearly describe all individuals' roles in fulfilling responsibilities under the Plan, including back-up contacts and escalation pathways;

   iii. require regular testing and review of the Plan, and the evaluation and revision of the Plan in light of such testing and review; and

   iv. require that once UBER has determined that an incident is a Data Security Incident, (a) a duly licensed attorney shall decide whether notification is required under applicable law; (b) that determination shall be documented in writing and communicated to UBER's Security Executive and to a member of UBER's legal department with a supervisory role at least at the level of associate general counsel; (c) UBER shall maintain documentation sufficient to show the investigative and responsive actions taken in connection with the Data Security Incident and the determination as to whether notification is required; and (d) UBER shall assess whether there are reasonably feasible training or technical measures, in addition to those already in place, that would materially decrease the risk of the same

type of Data Security Incident re-occurring. UBER's Security Executive is responsible for overseeing, maintaining and implementing the Plan.

c. UBER's Security Executive shall report to the Chief Executive Officer, the Chief Legal Officer, and the Board of Directors on a quarterly basis how many Data Security Incidents occurred and how they were resolved, including any payment by UBER in excess of $5,000 to a third party who reported the Data Security Incident to UBER such as through a bug bounty program (other than a payment to a forensics company retained by UBER).

16. Corporate Integrity Program

a. UBER shall develop, implement, and maintain a hotline or equivalent mechanism for employees to report misconduct, ethical concerns, or violations of UBER's policies, cultural norms, or code of conduct.

b. UBER shall require an executive or officer with appropriate background and experience in compliance to report to the Board of Directors, or to a committee thereof, at each regularly scheduled meeting of the Board of Directors or committee to provide information concerning instances or allegations of misconduct, ethical concerns, or violations of UBER's policies, cultural norms, or code of conduct, including complaints received by the hotline.

c. No later than ninety (90) days after the Effective Date and for a period of ten (10) years thereafter, UBER shall develop, implement and maintain a process, incorporating privacy by design principles, to review proposed changes to UBER's applications, its products, and any other ways in which UBER uses, collects, or shares data collected from or about Riders and Drivers.

d. UBER shall develop, implement, and maintain an annual training program for employees concerning UBER's code of conduct.

e. UBER's Security Executive shall advise the Chief Executive Officer or the Chief Legal Officer of UBER's security posture, security risks faced by UBER, and security implications of UBER's business decisions.

Meet and Confer

17. If the Attorney General reasonably believes that UBER has failed to comply with any of Paragraphs 12 through 16 of this Final Judgment and Consent Decree, and if in the Attorney General's sole discretion the failure to comply does not threaten the health or safety of citizens and does not create an emergency requiring immediate action, the Attorney General will notify UBER in writing of such failure to comply and UBER shall have thirty (30) days from receipt of such written notice to provide a good faith written response, including either a statement that UBER believes it is in full compliance or otherwise a statement explaining how the violation occurred, how it has been addressed or when it will be addressed, and what UBER will do to make sure the violation does not happen again. The Attorney General may agree to provide UBER more than thirty (30) days to respond.

18. Nothing herein shall be construed to exonerate any failure to comply with any provision of this Final Judgment and Consent Decree, or to compromise the authority of the Attorney General to initiate a proceeding for any failure to comply with this Final Judgment and Consent Decree in the circumstances excluded in Paragraph 17 or if, after receiving the response from UBER described in Paragraph 17, the Attorney General determines that an enforcement action is in the public interest.

Payment to the States

19. Within thirty (30) days of the Effective Date, UBER shall pay **One Hundred Forty-Eight Million Dollars ($148,000,000)** to the Attorneys General, to be distributed as agreed by the Attorneys General with $2,620,711.81 to be paid by UBER to the District of Columbia. If the Court has not entered this Final Judgment and Consent Decree by the Effective Date, UBER shall pay within thirty (30) days of the Effective Date or within fourteen (14) days of entry of this Final Judgment and Consent Decree, whichever is later. The money received by the District of Columbia may be used for purposes that may include, but are not limited to, attorneys' fees, and other costs of investigation and litigation, or be placed in, or applied to, the District's restitution fund or litigation support fund, used to defray the costs of the inquiry leading hereto, or for other uses permitted by state law, at the sole discretion of the Attorney General for the District of Columbia. UBER agrees to cooperate with the District in obtaining any modification to the language of this paragraph needed to facilitate the administration of the District's payment under this paragraph.

Release

20. Upon payment of the amount due to the District of Columbia under this Final Judgment and Consent Decree, the Attorney General shall release and discharge UBER from all civil claims that the Attorney General could have brought under the CPPA and the CSBNA or common law claims concerning unfair, deceptive, or fraudulent trade practices based on the Covered Conduct. Nothing contained in this paragraph shall be construed to limit the ability of the Attorney General to enforce the obligations that UBER has under this Final Judgment and Consent Decree. Further, nothing in this Final

Judgment and Consent Decree shall be construed to create, waive, or limit any private right of action.

General Provisions

21. The parties understand and agree that this Final Judgment and Consent Decree shall not be construed as an approval or a sanction by the Attorney General of UBER's business practices, nor shall UBER represent that this Final Judgment and Consent Decree constitutes an approval or sanction of its business practices. The parties further understand and agree that any failure by the Attorney General to take any action in response to any information submitted pursuant to this Final Judgment and Consent Decree shall not be construed as an approval or sanction of any representations, acts, or practices indicated by such information, nor shall it preclude action thereon at a later date.
22. Nothing in this Final Judgment and Consent Decree shall be construed as relieving UBER of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of the provisions of this Final Judgment and Consent Decree be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.
23. UBER shall deliver a copy of this Final Judgment and Consent Decree to, or otherwise fully apprise, its executive management having decision-making authority with respect to the subject matter of this Final Judgment and Consent Decree within thirty (30) days of the Effective Date.
24. To the extent that there are any, UBER agrees to pay all court costs associated with the filing (if legally required) of this Final Judgment and Consent Decree. No court costs, if any, shall be taxed against the Attorney General.

25. If any clause, provision, paragraph, or section of this Final Judgment and Consent Decree is for any reason held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, paragraph, or section of this Final Judgment and Consent Decree, and this Final Judgment and Consent Decree shall be construed and enforced as if such illegal, invalid, or unenforceable clause, provision, paragraph, or section had not been contained herein.

Any notice or report provided by UBER to the Attorney General under this Final Judgment and Consent Decree shall be satisfied by sending notice to the Designated Contacts in *Appendix B.* Any notice or report provided by the Attorney General to UBER under this Final Judgment and Consent Decree shall be satisfied by sending notice to: Chief Legal Officer, Uber Technologies, Inc., 1455 Market Street, San Francisco, California 94103; with a copy to Rebecca S. Engrav, Perkins Coie LLP, 1201 Third Avenue, Suite 4900, Seattle, Washington 98101. All such notices or reports shall be sent by United States mail, certified mail return receipt requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the notice or document, and shall be deemed to be sent upon mailing. Notwithstanding the foregoing, if a sending party requests of the receiving party whether transmission by electronic mail is sufficient for a particular notice or report and the receiving party agrees, electronic mail may be used if an electronic return receipt is provided. An Attorney General may update its address by sending a complete, new updated version of *Appendix B* to UBER and to all other Attorneys General listed on *Appendix B.* UBER may update its address by sending written notice to all parties listed in *Appendix B.*

APPROVED:

PLAINTIFF, THE DISTRICT OF COLUMBIA

KARL A. RACINE
Attorney General for the District of Columbia

_____ Date:_____

Benjamin Wiseman
Director, Office of Consumer Protection
Office of the Attorney General
441 Fourth Street, N.W., Suite 600 South
Washington, D.C. 20001

APPROVED:

DEFENDANT, UBER TECHNOLOGIES, INC.

By: _____ Date: _____
Tony West
Chief Legal Officer

APPROVED:

COUNSEL FOR DEFENDANT, UBER TECHNOLOGIES, INC.

By: _____ Date: _____
John K. Roche (D.C. Bar # 491112)
Perkins Coie LLP
700 13th St. N.W., Suite 600
Washington, DC 20005-3960
Telephone: 202-434-1627
Fax: 202-654-9106
Email: JRoche@perkinscoie.com
Local Counsel for Uber Technologies, Inc.

Rebecca S. Engrav
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
Telephone: (206) 359-6168
Email: rengrav@perkinscoie.com
Lead Counsel for Uber Technologies, Inc.

Entered:

_____ Date: _____
Judge