THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

JOSHUA R. DIAMOND
DEPUTY ATTORNEY GENERAL

WILLIAM E. GRIFFIN
CHIEF ASST. ATTORNEY GENERAL

STATE OF VERMONT
OFFICE OF THE ATTORNEY GENERAL
109 STATE STREET
MONTPELIER, VT
05609-1001

TEL: (802) 828-3171
FAX: (802) 828-3187

http://www.ago.vermont.gov

November 14, 2018

Via Email to greg.bensinger@wsj.com
Greg Bensinger
The Wall Street Journal
201 California St., Suite 1100
San Francisco, CA 94111

Re: Public Records Request

Dear Mr. Bensinger:

I write in response to your public records act request dated October 30, 2018.

You requested "copies of all communications digital or physical between the attorney general's office and Uber Technologies Inc. regarding Uber's 2016 breach affecting customer and driver data and its subsequent settlement."

Please find documents responsive to your request attached. Please be advised that we have withheld records that are exempt from disclosure pursuant to 1 V.S.A. § 317(c)(4).

To the extent you feel information has been withheld in error, you may appeal to the Deputy Attorney General, Joshua Diamond. Thank you.

Sincerely,

Christopher J. Curtis
Chief, Public Protection Division

Cornell-Brown, Rowan

From: Haney, Rachel (Perkins Coie) <RHaney@perkinscoie.com>
Sent: Monday, September 24, 2018 4:36 PM
To: Kriger, Ryan
Cc: Elizabeth Blackston; Matt Van Hise (MVanHise@atg.state.il.us); Engrav, Rebecca S. (Perkins Coie); Spear, Ryan M. (Perkins Coie)
Subject: Vermont Uber Consent Judgment: Final Documents
Attachments: UDB – VERMONT Judgment – FINAL.DOCX; UDB – VERMONT – FINAL Signatures.PDF

Good afternoon. Attached are Word copies of the final documents for your state, as agreed by the parties. The necessary signature pages are also attached.

Important note: The documents should match everything previously shared and discussed with you, but we would appreciate your help to make sure that is the case. Please review them carefully to confirm that they incorporate all changes from both sides and that you confirm this is the final version. If there is an issue, please bring that to our attention as quickly as possible.

Hard copies: If you are one of the following states, we are also sending you hard copies of the ink signature pages by overnight mail. (In a few instances, local counsel's signature will come in a separate packet tomorrow directly from local counsel.) You should receive them tomorrow; please let us know if you do not. If you are **not** on this list but want hard copy signature pages, please reply immediately to let us know. *States receiving hard copy signature pages: Alabama, Alaska, Arkansas, California, Colorado, Georgia, Hawaii, Illinois, Indiana, Kentucky, Louisiana, Maine, Massachusetts, Michigan, Mississippi, Montana, Nebraska, New Hampshire, New Jersey, North Carolina, North Dakota, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Utah, Vermont, Virginia, Washington, West Virginia, Wyoming.*

Filing fees, now: If you are one of the following states, we have processed and are sending you a check for filing fees by overnight mail. You should receive it tomorrow; please let us know if you do not. *States receiving filing fees now: Arkansas, California, Indiana (*wire transfer not check), Mississippi, South Carolina, Tennessee, Wyoming.*

Filing fees, later: If you are one of the following states, we have you on our list for filing fee reimbursement after filing. We'll be in touch with you to confirm details at a later date. *States receiving filing fees later: Georgia, Iowa, Louisiana, Nebraska, New York, North Carolina, Ohio, Oregon, Pennsylvania, Texas, Utah, West Virginia.*

Thank you very much for your hard work and professionalism on this matter. It has been a pleasure working with you. We are excited to see it go over the finish line.

Warm regards,

Rachel Haney | **Perkins Coie LLP**
ASSOCIATE
1201 Third Avenue Suite 4900
Seattle, WA 98101-3099
D. +1.206.359.8544
F. +1.206.359.9544
E. RHaney@perkinscoie.com

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

STATE OF VERMONT, Plaintiff	)	CIVIL DIVISION Docket No. _____
v.	)	
UBER TECHNOLOGIES, INC. Defendant	)	

FINAL JUDGMENT AND CONSENT DECREE

Plaintiff, the State of Vermont, by Thomas J. Donovan, Jr., Attorney General of the State of Vermont, has filed a Complaint for a permanent injunction and other relief in this matter pursuant to the Vermont Consumer Protection Act, 9 V.S.A. §§ 2451 et seq. ("CPA") and the Security Breach Notice Act, 9 V.S.A. § 2435 (the "Notice Act"), alleging Defendant, UBER TECHNOLOGIES, INC. ("UBER") committed violations of the CPA and the Notice Act.

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, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New

[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.

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 charged with enforcement of the CPA and Notice Act.
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.

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 Vermont, in that UBER is a technology company that

[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.*

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 same meaning as "Personally Identifiable Information" as set forth in 9 V.S.A. § 2430(5).
6. "Riders and Drivers" or, as applicable, "Rider or Driver" shall mean any individual natural person who is a resident of Vermont 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 the CPA and Notice Act. 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 CPA and Notice Act 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 Notice Act.

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 Vermont 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 Vermont 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. 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 Attorneys General pursuant to this paragraph 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, any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, litigation or local consumer aid fund or revolving 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 Attorneys General, and in Vermont, pursuant to the Constitution of the State of Vermont, Ch. II § 27 and 32 V.S.A. § 462.

20. The Office of the Vermont Attorney General has determined that the State of Vermont's award in this matter is the total amount of $ 587,219.91 and shall include: $18,200.00 for

payments to the Vermont drivers pursuant to 9 V.S.A. § 2458(b)(2) who received notice in November 2017 that their information was the subject of the Covered Conduct.

Release

21. Upon payment of the amount due to Vermont 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 CPA or Notice Act 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

22. 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.
23. 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.

24. 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.

25. 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.

26. 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.

27. 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, STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____ Date: _____

Ryan G. Kriger
Assistant Attorney General
Office of Attorney General
109 State Street
Montpelier, Vermont 05609
ryan.kriger@vermont.gov
802-828-3170

[Additional approvals on subsequent pages]

APPROVED:

DEFENDANT, UBER TECHNOLOGIES, INC.

By: _____ Date: _____
Tony West
Chief Legal Officer

APPROVED:

COUNSEL FOR DEFENDANT, UBER TECHNOLOGIES, INC.

By: _____ Date: _____

Jonathan Rose [ERN 6128]
Dunkiel Saunders Elliott Raubvogel & Hand PLLC
91 College Street, PO Box 545
Burlington, VT 05402-0545
Telephone: 802-860-1003 x 117
Email: jrose@dunkielsaunders.com
Local Counsel for Uber Technologies, Inc.

Rebecca S. Engrav (Not Admitted *Pro Hac Vice*)
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

APPROVED:

DEFENDANT, UBER TECHNOLOGIES, INC.

By: _____ Date: 9.21.18
Tony West
Chief Legal Officer

APPROVED:

COUNSEL FOR DEFENDANT, UBER TECHNOLOGIES, INC.

By: _____ Date: 9/21/18

Jonathan Rose [ERN 6128]
Dunkiel Saunders Elliott Raubvogel & Hand PLLC
91 College Street, PO Box 545
Burlington, VT 05402-0545
Telephone: 802-860-1003 x 117
Email: jrose@dunkielsaunders.com
Local Counsel for Uber Technologies, Inc.

Rebecca S. Engrav (Not Admitted *Pro Hac Vice*)
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

Cornell-Brown, Rowan

From: Kriger, Ryan
Sent: Thursday, September 27, 2018 10:18 AM
To: REngrav@perkinscoie.com; RHaney@perkinscoie.com; RSpear@perkinscoie.com
Cc: MVanHise@atg.state.il.us; EBlackston@atg.state.il.us
Subject: Vermont -- Uber Filing
Attachments: Uber Consent Decree FILED.pdf; Uber Complaint FILED.pdf

Attached please find Vermont's file-stamped copy of the Uber Complaint and Consent Decree. We will forward the court-approved document when we receive it.

-Ryan

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

STATE OF VERMONT, Plaintiff	)	CIVIL DIVISION Docket No. 540-9-18 Wncv.
v.	)	
UBER TECHNOLOGIES, INC. Defendant	)	

FINAL JUDGMENT AND CONSENT DECREE

Plaintiff, the State of Vermont, by Thomas J. Donovan, Jr., Attorney General of the State of Vermont, has filed a Complaint for a permanent injunction and other relief in this matter pursuant to the Vermont Consumer Protection Act, 9 V.S.A. §§ 2451 et seq. ("CPA") and the Security Breach Notice Act, 9 V.S.A. § 2435 (the "Notice Act"), alleging Defendant, UBER TECHNOLOGIES, INC. ("UBER") committed violations of the CPA and the Notice Act.

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, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New

[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.

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 charged with enforcement of the CPA and Notice Act.
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.

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 Vermont, in that UBER is a technology company that

[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.*

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 same meaning as "Personally Identifiable Information" as set forth in 9 V.S.A. § 2430(5).
6. "Riders and Drivers" or, as applicable, "Rider or Driver" shall mean any individual natural person who is a resident of Vermont 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 the CPA and Notice Act. 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 CPA and Notice Act 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 Notice Act.

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 Vermont 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 Vermont 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. 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 Attorneys General pursuant to this paragraph 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, any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, litigation or local consumer aid fund or revolving 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 Attorneys General, and in Vermont, pursuant to the Constitution of the State of Vermont, Ch. II § 27 and 32 V.S.A. § 462.

20. The Office of the Vermont Attorney General has determined that the State of Vermont's award in this matter is the total amount of $ 587,219.91 and shall include: $18,200.00 for

payments to the Vermont drivers pursuant to 9 V.S.A. § 2458(b)(2) who received notice in November 2017 that their information was the subject of the Covered Conduct.

Release

21. Upon payment of the amount due to Vermont 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 CPA or Notice Act 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

22. 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.
23. 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.

24. 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.

25. 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.

26. 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.

27. 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, STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____ Date: 9/25/2018

Ryan G. Kriger
Assistant Attorney General
Office of Attorney General
109 State Street
Montpelier, Vermont 05609
ryan.kriger@vermont.gov
802-828-3170

[Additional approvals on subsequent pages]

APPROVED:

DEFENDANT, UBER TECHNOLOGIES, INC.

By: _____ Date: 9.21.18
Tony West
Chief Legal Officer

APPROVED:

COUNSEL FOR DEFENDANT, UBER TECHNOLOGIES, INC.

By: _____ Date: 9/21/18

Jonathan Rose [ERN 6128]
Dunkiel Saunders Elliott Raubvogel & Hand PLLC
91 College Street, PO Box 545
Burlington, VT 05402-0545
Telephone: 802-860-1003 x 117
Email: jrose@dunkielsaunders.com
Local Counsel for Uber Technologies, Inc.

Rebecca S. Engrav (Not Admitted *Pro Hac Vice*)
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

Appendix A.

STATE	CONSUMER PROTECTION ACTS and PERSONAL INFORMATION PROTECTION ACTS
Alabama	Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-1, *et seq.*; Alabama Data Breach Notification Act of 2018, Ala. Code § 8-38-1, *et seq.*
Alaska	The Alaska Unfair Trade Practices and Consumer Protection Act, AS 45.50.471 *et seq.*; The Alaska Personal Information Protection Act, AS 45.48 *et seq.*
Arizona	Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-1521 *et seq.*; Arizona Data-Breach Notification Law, Ariz. Rev. Stat. § 18-545 (in effect 2016-2018; now codified, as revised, at Ariz. Rev. Stat. §§ 18-551 and 18-552)
Arkansas	Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-101, *et seq.*; Personal Information Protection Act, Ark. Code Ann. §§ 4-110-101, *et seq.*
California	California Business & Professions Code, section 17200, *et seq.*; California Civil Code, sections 1798.82 and 1798.81.5
Colorado	Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-101, *et seq.*
Connecticut	Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110a *et seq.*; Breach of Security re Computerized Data Containing Personal Information, Conn. Gen. Stat. § 36a-701b; Safeguarding of Personal Information, Conn. Gen. Stat. § 42-471
District of Columbia	D.C. Code §§ 28-3901, *et seq.*; D.C. Code §§ 28-3851, *et seq.*
Delaware	Delaware Consumer Fraud Act, 6 Del. C. § 2511, *et seq.*; Delaware Uniform Deceptive Trade Practices Act, 6 Del. C. § 2531, *et seq.*; Delaware Computer Security Breaches Act, 6 Del. C.§ 12B-100, *et seq.*

Appendix A.

Florida	Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, Florida Statutes; Florida Information Protection Act, Section 501.171, Florida Statutes
Georgia	Fair Business Practices Act, O.C.G.A. §§ 10-1-390 through 408; Georgia Personal Identity Protection Act, O.C.G.A. §§ 10-1-910 through 912
Hawaii	Monopolies; Restraint of Trade, Haw. Rev. Stat. Chpt. 480; Security Breach of Personal Information, Haw. Rev. Stat. Chpt. 487N
Idaho	Idaho Consumer Protection Act, Idaho Code §§ 48-601 *et seq.*; Idaho Identity Theft Act, Idaho Code §§ 28-51-101 *et seq.*
Illinois	Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*; Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.*
Indiana	Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq.*; Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq.*
Iowa	Iowa Consumer Fraud Act, Iowa Code § 714.16; Personal Information Security Breach Protection, Iowa Code § 715C
Kansas	Kansas Consumer Protection Act K.S.A. 50-623 *et seq.*; Wayne Owen Act K.S.A. 50-6,139b
Kentucky	Kentucky Consumer Protection Act, KRS 367.110-.300 and 367.990; KRS 365.732
Louisiana	Unfair Trade Practices and Consumer Protection Law LA RS 51:1401 *et seq.*; Database Security Breach Notification Law LA RS 51:3071 *et seq.*
Maine	Maine Unfair Trade Practices Act, 5 M.R.S.A. §§ 205-A through 214; Maine Notice of Risk to Personal Data Act, 10 M.R.S.A. §§ 1346 through 1350-B

Appendix A.

Maryland	Maryland Consumer Protection Act, Md. Code Ann., Com. Law § 13-101, *et seq.* (2013 Repl. Vol and 2017 Supp.); Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3501, *et seq.* (2013 Repl. Vol and 2017 Supp.)
Massachusetts	Massachusetts Consumer Protection Act (G.L. c. 93A); Massachusetts Data Security Law (G.L. c. 93H)
Michigan	Michigan Consumer Protection Act, MCL 445.901, *et seq.*; Michigan Identity Theft Protection Act, MCL 445.61, *et seq.*
Minnesota	Minnesota Deceptive Trade Practices Act, Minn. Stat. §§ 325D.43 *et seq.* Minnesota Prevention of Consumer Fraud Act, Minn. Stat. §§ 325F.68 *et seq.* Minnesota Data Breach Notification Statute, Minn. Stat. § 325E.61.
Mississippi	Mississippi Consumer Protection Act Miss. Code Ann. § 75-24-1 *et seq.*; Notice of Breach of Security Miss. Code Ann. § 75-24-29
Missouri	Mo. Rev. Stat. § 407.010, *et seq.*; Mo. Rev. Stat. § 407.1500
Montana	Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. §§ 30-14-101 *et seq.*; Montana Impediment of Identity Theft Act, Mont. Code Ann. §§ 30-14-1701 *et seq.*
Nebraska	Consumer Protection Act, Neb. Rev. Stat. § 59-1601 *et seq.*; Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301 *et seq.*; Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. § 87-801 *et seq.*
Nevada	Nevada Deceptive Trade Practices Act; Nev. Rev. Stat. §§ 598.0903, *et seq.*; Nevada Security of Personal Information Act; Nev. Rev. Stat. §§ 603A.010, *et seq.*
New Hampshire	NH RSA 358-A; NH RSA 359-C: 19-21

Appendix A.

New Jersey	New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 *et seq.*; New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166
New Mexico	The New Mexico Unfair Practices Act, NMSA 1978, §§ 57-12-1 to -26 (1967, as amended through 2009); The New Mexico Data Breach Notification Act, NMSA 1978, §§ 57-12C-1 to -12 (2017)
New York	Executive Law 63(12) and General Business Law 349/350
North Carolina	North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. §§ 75-1.1, *et seq.*; North Carolina Identity Theft Protection Act, N.C. Gen. Stat. §§ 75-60, *et seq.*
North Dakota	Unlawful Sales or Advertising Practices N.D.C.C. § 51-15-01 *et seq.*; Notice of Security Breach for Personal Information N.D.C.C. § 51-30-01 *et seq.*
Ohio	Ohio Consumer Sales Practices Act, Ohio R.C. 1345.01 *et seq.*; Ohio Data Breach Notification Act, R.C. 1349.19 *et seq.*
Oklahoma	Oklahoma Consumer Protection Act, 15 O.S. §§ 751 *et seq.*; Security Breach Notification Act, 24 O.S. §§ 161 *et seq.*
Oregon	Unlawful Trade Practices Act, ORS 646.605 *et seq.*; Oregon Consumer Identity Theft Protection Act, ORS 646A.600 *et seq.*
Pennsylvania	Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1 – 201-9.3; Breach of Personal Information Notification Act, 73 P.S. § 2301, *et seq.*
Rhode Island	Rhode Island Gen. Laws § 6-13.1-1, *et seq.*; Rhode Island Gen. Laws § 11-49.3-1, *et seq.*
South Carolina	South Carolina Unfair Trade Practices Act §§39-5-10 *et seq.*; Section 39-1-90
South Dakota	SDCL 37-24; Data Breach Notification SDCL 22-40-19 through 22-40-26

Appendix A.

Tennessee	Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. §§ 47-18-101 to -131; Tennessee Identity Theft Deterrence Act of 1999, §§ 47-18-2101 to -2111
Texas	Deceptive Trade Practices – Consumer Protection Act, Tex. Bus. & Com. Code Ann.§§ 17.41-17.63; Identity Theft Enforcement and Protection Act, Tex. Bus. & Com. Code Ann. § 521.001 -152
Utah	Utah Consumer Sales Practices Act, Utah Code §§ 13-11-1, *et. seq.*; Utah Protection of Personal Information Act, Utah Code §§ 13-44-101, *et. seq.*
Vermont	Vermont Consumer Protection Act, 9 V.S.A. §§ 2451 *et seq.*; Vermont Security Breach Notice Act, 9 V.S.A. § 2435
Virginia	Breach of Personal Information Notification, Virginia Code § 18.2-186.6
Washington	Consumer Protection Act, RCW 19.86.020; Notice of Security Breaches law, RCW 19.255.010
West Virginia	West Virginia Consumer Credit and Protection Act, W.Va. Code § 46A-1-101 *et seq.*; Theft of Consumer Identity Protections, W.Va. Code § 46A-2A-101 *et seq.*
Wisconsin	Fraudulent Misrepresentations, Wis. Stat.§ 100.18; Notice of unauthorized acquisition of personal information, Wis. Stat. § 134.98
Wyoming	Wyoming Consumer Protection Act, Wyo. Stat. Ann. §§ 40-12-101 through -114; Wyo. Stat. Ann. §§ 40-12-501 through -509

Appendix B.

STATE	ATTORNEYS GENERAL DESIGNATED CONTACTS
Alabama	Michael G. Dean Assistant Attorney General Office of the Alabama Attorney General 501 Washington Avenue Montgomery, Alabama 36130 mdean@ago.state.al.us (334) 353-0415
Alaska	Cynthia A. Franklin Assistant Attorney General Office of the Alaska Attorney General 1031 W. 4th Ave, Suite 200 Anchorage, AK 99501 cynthia.franklin@alaska.gov (907) 269-5208
Arizona	John C. Gray Senior Litigation Counsel Arizona Attorney General's Office 2005 N. Central Ave. Phoenix, AZ 85004 john.gray@azag.gov (602) 542-7753
Arkansas	Peggy Johnson Assistant Attorney General Office of the Arkansas Attorney General 323 Center St., Suite 200 Little Rock, AR 72201 Peggy.johnson@arkansasag.gov (501) 682-8062
California	Lisa B. Kim Deputy Attorney General Office of the California Attorney General 300 S. Spring Street, Suite 1702 Los Angeles, CA 90013 Lisa.Kim@doj.ca.gov (213) 269-6369
Colorado	Mark T. Bailey Senior Assistant Attorney General Colorado Attorney General's Office 1300 Broadway, 7th Floor Denver, Colorado 80203 mark.bailey@coag.gov (720) 508-6202

Appendix B.

Connecticut	Jeremy Pearlman Assistant Attorney General Office of the Connecticut Attorney General 110 Sherman Street Hartford CT 06105 Jeremy.pearlman@ct.gov (860) 808-5440
District of Columbia	Benjamin Wiseman Director, Office of Consumer Protection Office of the District of Columbia Attorney General 441 4th Street NW, Suite 600S Washington, D.C. 20001 benjamin.wiseman@dc.gov (202) 741-5226
Delaware	Christian Douglas Wright Director of Consumer Protection Delaware Department of Justice 820 N. French Street Wilmington, DE 19801 christian.wright@state.de.us (302) 577-8944
Florida	Edward Moffitt Senior Financial Investigator Multistate and Privacy Bureau Florida Office of the Attorney General 135 W Central Boulevard Orlando, FL 32801-2437 Edward.Moffitt@myfloridalegal.com (407) 845-6388
Georgia	Melissa M. Devine Assistant Attorney General Office of the Georgia Attorney General 2 Martin Luther King, Jr. Drive, Suite 356 Atlanta, GA 30334 mdevine@law.ga.gov (404) 656-3795
Hawaii	Lisa P. Tong Enforcement Attorney State of Hawaii Office of Consumer Protection 235 S. Beretania Street #801 Honolulu, HI 96813 ltong@dcca.hawaii.gov (808) 586-2636

Appendix B.

Idaho	Jane E. Hochberg Deputy Attorney General Idaho Office of Attorney General Consumer Protection Division 954 W. Jefferson Street, 2nd Floor Boise, ID 83720-0010 Jane.Hochberg@ag.idaho.gov (208) 332-3553
Illinois	Matthew W. Van Hise, CIPP/US Assistant Attorney General Chief, Privacy Unit 500 South Second Street Springfield, IL 62701 mvanhise@atg.state.il.us (217) 782-9024
Indiana	Douglas Swetnam Section Chief, Data Privacy & Identity Theft Unit Office of the Indiana Attorney General 302 W. Washington St., IGCS – 5th Floor, Indianapolis, IN 46204 douglas.swetnam@atg.in.gov (317) 232-6294
Iowa	William R. Pearson Assistant Attorney General Office of the Attorney General of Iowa 1305 E. Walnut Street Des Moines, IA 50319 William.Pearson@ag.iowa.gov (515) 242-6773
Kansas	Sarah M. Dietz Assistant Attorney General Office of Kansas Attorney General 120 SW 10th Avenue, 2nd Floor Topeka, Kansas 66612 sarah.dietz@ag.ks.gov (785) 296-3751
Kentucky	Kevin R. Winstead Assistant Attorney General Kentucky Attorney General 1024 Capital Center Dr., #200 Frankfort, KY 40601 kevin.winstead@ky.gov (502) 696-5379

Appendix B.

Louisiana	Alberto A. De Puy Assistant Attorney General Louisiana Department of Justice 1885 N. Third Street, 4th Floor Baton Rouge, LA 70802 depuya@ag.louisiana.gov (225) 326-6471
Maine	Brendan O'Neil Assistant Attorney General Office of the Maine Attorney General 6 State House Station Augusta, ME 04333 brendan.oneil@maine.gov (207) 626-8842
Maryland	Richard L. Trumka Jr. Assistant Attorney General Consumer Protection Division Office of the Maryland Attorney General 200 St. Paul St. Baltimore, MD 21202 rtrumka@oag.state.md.us (410) 576-6957
Massachusetts	Sara Cable Director, Data Privacy & Security Assistant Attorney General Massachusetts Attorney General's Office One Ashburton Place Boston MA 02108 sara.cable@state.ma.us (617) 963-2827
Michigan	Kathy Fitzgerald Assistant Attorney General Corporate Oversight Division Michigan Department of Attorney General 525 W. Ottawa St. 6th Floor Lansing, MI 48933 fitzgeraldk@michigan.gov (517) 241-0026
Minnesota	Alex K. Baldwin Assistant Attorney General Minnesota Attorney General's Office 445 Minnesota Street St. Paul, MN 55101 alex.baldwin@ag.state.mn.us

Appendix B.

	(651) 757-1020
Mississippi	Crystal Utley Secoy Special Assistant Attorney General Mississippi Attorney General's Office PO Box 22947 Jackson, Mississippi 39225 cutle@ago.state.ms.us (601) 359-4213
Missouri	Michael Schwalbert Assistant Attorney General Missouri Attorney General's Office 815 Olive Street, Suite 200 Saint Louis, Missouri 63101 michael.schwalbert@ago.mo.gov (314) 340-7888
Montana	Mark W. Mattioli Chief, Office of Consumer Protection Montana Department of Justice 555 Fuller Avenue Helena, MT 59601 mmattioli@mt.gov (404) 444-5791
Nebraska	Dan Birdsall Assistant Attorney General Consumer Protection Division Nebraska Attorney General's Office 2115 State Capitol Lincoln, NE 68509 dan.birdsall@nebraska.gov (402) 471-3840
Nevada	Laura Tucker Senior Deputy Attorney General Office of the Nevada Attorney General 100 N. Carson Street Carson City, NV 89701 lmtucker@ag.nv.gov (775) 684-1244
New Hampshire	James T. Boffetti Associate Attorney General NH Department of Justice 33 Capitol Street Concord, NH 03301 james.boffetti@doj.nh.gov (603) 271-0302

Appendix B.

New Jersey	Elliott M. Siebers Deputy Attorney General Office of the New Jersey Attorney General 124 Halsey Street, 5th Floor P.O. Box 45029-5029 Newark, New Jersey 07101 elliott.siebers@law.njoag.gov (973) 648-4460
New Mexico	Brian E. McMath Assistant Attorney General Office of the New Mexico Attorney General 201 3rd St. NW, Suite 300 Albuquerque NM, 87102 bmcmath@nmag.gov (505) 717-3531
New York	Clark Russell Deputy Bureau Chief New York State Office of the Attorney General 28 Liberty Street New York, NY 10005 clark.russell@ag.ny.gov (212) 416.6494
North Carolina	Kim D'Arruda Special Deputy Attorney General North Carolina Department of Justice 114 West Edenton Street Raleigh, NC 27603 kdarruda@ncdoj.gov (919) 716-6000
North Dakota	Parrell D. Grossman Director, Consumer Protection & Antitrust Division Office of Attorney General of North Dakota 1050 East Interstate Ave. Ste. 200 Bismarck, ND 58503-5574 pgrossman@nd.gov (701) 328-5570
Ohio	Melissa Szozda Smith Senior Assistant Attorney General Office of the Ohio Attorney General 30 E. Broad Street, Floor 14 Columbus, OH 43215 melissa.s.smith@ohioattorneygeneral.gov

Appendix B.

	(614) 466.1305
Oklahoma	Julie A. Bays Chief, Consumer Protection Oklahoma Attorney General's Office 313 NE 21st Street Oklahoma City, OK 73105 julie.bays@oag.ok.gov (405) 522-3082
Oregon	Katherine A. Campbell Senior Assistant Attorney General Oregon Department of Justice 100 SW Market Street Portland, OR 97201-5702 katherine.campbell@doj.state.or.us (971) 673-1880
Pennsylvania	John M. Abel Senior Deputy Attorney General Office of the Pennsylvania Attorney General 15th Floor, Strawberry Square Harrisburg, PA 17120 jabel@attorneygeneral.gov (717) 783.1439
Rhode Island	Edmund F. Murray, Jr. Special Assistant Attorney General Rhode Island Department of Attorney General 150 South Main Street Providence, Rhode Island 02903 emurray@riag.ri.gov (401) 274-4400 ext. 2401
South Carolina	Chantelle Neese Assistant Attorney General South Carolina Attorney General's Office 1000 Assembly Street Columbia, SC 29201 cneese@scag.gov (803) 734-2346
South Dakota	Philip D. Carlson Assistant Attorney General South Dakota Attorney General 1302 E. Hwy. 14, Ste. 1 Pierre, SD 57501 Phil.Carlson@state.sd.us (605) 773-3215
Tennessee	Carolyn Smith

Appendix B.

	Senior Assistant Attorney General Tennessee Attorney General's Office P.O.Box 20207 Nashville, TN 37202-0207 carolyn.smith@ag.tn.gov (615) 532-2578
Texas	D. Esther Chavez Senior Assistant Attorney General Office of the Texas Attorney General PO Box 12548, MC- 010 Austin, TX 78711-2548 esther.chavez@oag.texas.gov (512) 475-4628
Utah	David N. Sonnenreich Deputy Attorney General Office of the Utah Attorney General PO Box 140874 Salt Lake City, Utah 84114-0874 dsonnenreich@agutah.gov (801) 366-0132
Vermont	Ryan Kriger Assistant Attorney General Office of the Vermont Attorney General 109 State St. Montpelier, VT 05609 ryan.kriger@vermont.gov (802) 828-3170
Virginia	Gene Fishel Senior Assistant Attorney General Office of the Virginia Attorney General 202 North 9th Street Richmond, VA 23219 sfishel@oag.state.va.us (804) 786-3870
Washington	Tiffany Lee Assistant Attorney General Office of the Washington Attorney General 800 5th Avenue, Suite 2000 Seattle, WA 98104 tiffanyc@atg.wa.gov (206) 464-6098
West Virginia	Laurel K. Lackey Assistant Attorney General Office of the West Virginia Attorney General

Appendix B.

	269 Aikens Center Martinsburg, WV 25404 laurel.k.lackey@wvago.gov (304) 267-0239
Wisconsin	Lara Sutherlin Assistant Attorney General Wisconsin Department of Justice 17 West Main Street, PO Box 7857 Madison, WI 53707-7857 sutherlinla@doj.state.wi.us (608) 267-7163
Wyoming	Benjamin M. Burningham Senior Assistant Attorney General Office of the Wyoming Attorney General 2320 Capitol Ave. Cheyenne, WY 82002 ben.burningham@wyo.gov (307) 777-7847

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

STATE OF VERMONT, Plaintiff	)	CIVIL DIVISION Docket No. 540-9-18 Wncv
v.	)	
UBER TECHNOLOGIES, INC. Defendant	)	

CONSUMER PROTECTION COMPLAINT

The Vermont Attorney General brings this lawsuit against Uber Technologies, Inc. ("Uber" or "Defendant") under the Vermont Consumer Protection Act, 9 V.S.A. §§ 2451 et seq. ("CPA") and the Security Breach Notice Act, 9 V.S.A. § 2435 (the "Notice Act") for engaging in unfair and deceptive practices and failing to notify consumers as required by the Notice Act. The Attorney General seeks injunctive relief, civil penalties, fees and costs, and other appropriate relief for these violations of the CPA and Notice Act.

PARTIES, JURISDICTION AND RELATED MATTERS

1. Defendant is a Delaware corporation with its principal place of business at 1455 Market Street, San Francisco, California 94103.
2. As used herein, any reference to "Uber" or "Defendant" shall mean Uber Technologies, Inc., including all officers, directors, affiliates, subsidiaries and divisions, predecessors, successors and assigns doing business in the United States.
3. At all times relevant to this Complaint, Defendant did business in Vermont and provided services and collected payments from Vermont consumers, in that Uber is a technology company that provides a ride hailing mobile application that connects drivers with riders,

including in Vermont. Riders hail and pay drivers using the Uber platform.

4. The Vermont Attorney General (the "Attorney General") is authorized under the Vermont Consumer Protection Act, 9 V.S.A. § 2458(b), to sue to enforce the CPA's prohibitions on unfair and deceptive acts and practices in commerce.

5. This Court has personal jurisdiction over Defendant and is the proper venue for this action, based on the services sold and payments collected by Defendant from Vermont consumers, including in Washington County.

6. This action is in the public interest.

STATUTORY FRAMEWORK

7. The Vermont Consumer Protection Act, 9 V.S.A. § 2453(a), prohibits unfair and deceptive acts and practices in commerce.

8. The Vermont Security Breach Notice Act, 9 V.S.A. § 2435, requires and business that experiences a data security breach to notify consumers in the most expedient time possible and without unreasonable delay, but no more than 45 days after discovery or notification of the breach. It also requires that preliminary notice be provided to the Attorney General within 14 days of discovery or notification of the breach.

9. The acts described below, and summarized in paragraphs 10 to 18, constitute unfair and deceptive acts and practices in commerce and violate the CPA and the Notice Act.

BACKGROUND

10. In November 2016, hackers contacted Uber to inform them that they had accessed and acquired Uber data and to demand payment in exchange for deleting the data.

11. Uber was able to determine the security vulnerability that the hackers had exploited and eliminate the vulnerability.

12. In December 2016, the hackers deleted the data.

13. Among the data the hackers acquired was personal information pursuant to the Notice Act: name and driver's license information pertaining to some Uber drivers.

14. Uber did not disclose the data breach to the Attorney General or affected Uber drivers in 2016 when the breach was discovered.

15. In August 2017, Uber named a new CEO, Dara Khosrowshani.

16. In September 2017, Khosrowshani was informed that Uber had suffered a data breach and ordered an investigation into the data breach, hiring a third-party cyber security provider to conduct the investigation.

17. The cyber security provider verified the 2016 data breach, and, on November 21, 2017, Uber notified regulators and consumers of the 2016 breach.

18. Uber offered affected drivers free credit monitoring and identity theft protection.

First Cause of Action:
Unfair and Deceptive Trade Practices

19. Plaintiff realleges and incorporates by reference herein each and every allegation contained in the preceding paragraphs 1 through 18.

20. Defendant engaged in unfair and deceptive trade practices in commerce in violation of the Vermont Consumer Protection Act, 9 V.S.A. § 2453(a), including:

    a. failing to implement and maintain reasonable security practices to protect the sensitive personal information it maintains for its users;

    b. failing to disclose a data breach to affected users; and

    c. representing to users that Uber protects the sensitive personal information of its users, when in fact the hackers were able to gain access to some Uber user personal information.

Second Cause of Action:
Failure to Provide Timely Notice of a Security Breach

1. Plaintiff realleges and incorporates by reference herein each and every allegation contained in the preceding paragraphs 1 through 19.
2. Uber is a data collector pursuant to the Notice Act, 9 V.S.A. § 2430(3).
3. The Uber information the hackers acquired included Personally Identifiable Information pursuant to the Notice Act, 9 V.S.A. § 2430(5).
4. Uber violated the Notice Act, in that Uber suffered a breach of the security of its system data and failed to notify affected Vermont residents in the most expedient time possible and without unreasonable delay, but no more than 45 days after the discovery or notification of the breach.
5. Uber violated the Notice Act, in that Uber failed to notify the Attorney General within 14 days of the discovery or notification of the breach.

WHEREFORE, Plaintiff State of Vermont respectfully requests judgment in its favor and the following relief:

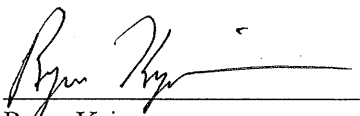
1. A judgment determining that Defendant has violated the Vermont Consumer Protection Act and the Security Breach Notice Act;
2. A permanent injunction prohibiting Defendant from further acts and practices in violation the Vermont Consumer Protection Act, or further violations of the Security Breach Notice Act;
3. Civil penalties for up to $10,000 for each violation of the Vermont Consumer Protection Act and for each violation of the Security Breach Notice Act;
4. The award of investigative and litigation costs and fees to the state of Vermont; and

5. Such other and further relief as the Court may deem appropriate.

Dated: September 25, 2018

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: 

Ryan Kriger
Assistant Attorneys General
Vermont Attorney General's Office
109 State Street
Montpelier, VT 05609
Tel. (802) 828-5479
ryan.kriger@vermont.gov

Cornell-Brown, Rowan

From: Haney, Rachel (Perkins Coie) <RHaney@perkinscoie.com>
Sent: Thursday, September 27, 2018 11:54 AM
To: Kriger, Ryan; Engrav, Rebecca S. (Perkins Coie); Spear, Ryan M. (Perkins Coie)
Cc: MVanHise@atg.state.il.us; EBlackston@atg.state.il.us
Subject: RE: Vermont -- Uber Filing

Ryan,

Confirming receipt. Thanks very much for sending.

Warm regards,

Rachel Haney | **Perkins Coie LLP**
ASSOCIATE
1201 Third Avenue Suite 4900
Seattle, WA 98101-3099
D. +1.206.359.8544
F. +1.206.359.9544
E. RHaney@perkinscoie.com

From: Kriger, Ryan [mailto:ryan.kriger@vermont.gov]
Sent: Thursday, September 27, 2018 7:18 AM
To: Engrav, Rebecca S. (SEA) <REngrav@perkinscoie.com>; Haney, Rachel A.S. (SEA) <RHaney@perkinscoie.com>; Spear, Ryan M. (SEA) <RSpear@perkinscoie.com>
Cc: MVanHise@atg.state.il.us; EBlackston@atg.state.il.us
Subject: Vermont -- Uber Filing

Attached please find Vermont's file-stamped copy of the Uber Complaint and Consent Decree. We will forward the court-approved document when we receive it.

-Ryan

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

Cornell-Brown, Rowan

From: Kriger, Ryan
Sent: Wednesday, October 3, 2018 5:27 PM
To: Engrav, Rebecca S. (Perkins Coie); Haney, Rachel (Perkins Coie); RSpear@perkinscoie.com
Cc: 'Van Hise, Matthew'; Blackston, Elizabeth
Subject: Fw: Docket No. 540-9-18 Wncv, State of Vermont vs. Uber Technologies, Inc., ORDER
Attachments: State of VT v. Uber Technologies; 540-9-18 Wncv.pdf

Counsel,

Attached please find the signed Order in the Vermont Uber matter.

Thank you for all of your work on this.

-Ryan

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001
ph: (802) 828-3170
ryan.kriger@vermont.gov

From: JUD - Washington Unit
Sent: Wednesday, October 3, 2018 4:31 PM
To: Kriger, Ryan
Cc: AGO - Consumer Info
Subject: Docket No. 540-9-18 Wncv, State of Vermont vs. Uber Technologies, Inc., ORDER

Please see the attached document: ORDER
Donna Waters
Washington Civil Division, Vermont Superior Court
65 State Street, Montpelier, Vermont 05602
Civil (802)828-2091^Small Claims (802)828-5551
www.vermontjudiciary.org
***** DO NOT REPLY ***** This email account is not monitored for responses. Please contact the court in person, by phone, or by U.S. mail if you need assistance.
***** CONFIDENTIAL ***** This email message and related attachments may contain personal and/or privileged information. If you are not the intended recipient, do not disseminate, distribute or copy this email message or any attachments. Please immediately notify JUD.Helpdesk@vermont.gov and permanently delete this email message and any attachments from your computer. For all other assistance, please contact the court.
EMAIL RECIPIENT INFORMATION:

RYAN G KRIGER (ryan.kriger@vermont.gov; ago.consumerinfo@vermont.gov)
Phone: (802)828-3170, ERN 4740

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

STATE OF VERMONT, Plaintiff	)	CIVIL DIVISION Docket No. 540-9-18 Wncv
v.	)	
UBER TECHNOLOGIES, INC. Defendant	)	

FINAL JUDGMENT AND CONSENT DECREE

Plaintiff, the State of Vermont, by Thomas J. Donovan, Jr., Attorney General of the State of Vermont, has filed a Complaint for a permanent injunction and other relief in this matter pursuant to the Vermont Consumer Protection Act, 9 V.S.A. §§ 2451 et seq. ("CPA") and the Security Breach Notice Act, 9 V.S.A. § 2435 (the "Notice Act"), alleging Defendant, UBER TECHNOLOGIES, INC. ("UBER") committed violations of the CPA and the Notice Act.

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, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New

[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.

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 charged with enforcement of the CPA and Notice Act.
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.

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 Vermont, in that UBER is a technology company that

[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.*

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 same meaning as "Personally Identifiable Information" as set forth in 9 V.S.A. § 2430(5).
6. "Riders and Drivers" or, as applicable, "Rider or Driver" shall mean any individual natural person who is a resident of Vermont 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 the CPA and Notice Act. 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 CPA and Notice Act 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 Notice Act.

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 Vermont 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 Vermont 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. 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 Attorneys General pursuant to this paragraph 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, any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, litigation or local consumer aid fund or revolving 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 Attorneys General, and in Vermont, pursuant to the Constitution of the State of Vermont, Ch. II § 27 and 32 V.S.A. § 462.

20. The Office of the Vermont Attorney General has determined that the State of Vermont's award in this matter is the total amount of $ 587,219.91 and shall include: $18,200.00 for

payments to the Vermont drivers pursuant to 9 V.S.A. § 2458(b)(2) who received notice in November 2017 that their information was the subject of the Covered Conduct.

Release

21. Upon payment of the amount due to Vermont 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 CPA or Notice Act 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

22. 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.
23. 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.

24. 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.

25. 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.

26. 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.

27. 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, STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____ Date: 9/25/2018

Ryan G. Kriger
Assistant Attorney General
Office of Attorney General
109 State Street
Montpelier, Vermont 05609
ryan.kriger@vermont.gov
802-828-3170

[Additional approvals on subsequent pages]

APPROVED:

DEFENDANT, UBER TECHNOLOGIES, INC.

By: _____ Date: 9.21.18
Tony West
Chief Legal Officer

APPROVED:

COUNSEL FOR DEFENDANT, UBER TECHNOLOGIES, INC.

By: _____ Date: 9/21/18

Jonathan Rose [ERN 6128]
Dunkiel Saunders Elliott Raubvogel & Hand PLLC
91 College Street, PO Box 545
Burlington, VT 05402-0545
Telephone: 802-860-1003 x 117
Email: jrose@dunkielsaunders.com
Local Counsel for Uber Technologies, Inc.

Rebecca S. Engrav (Not Admitted *Pro Hac Vice*)
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:

Mary Miles Teachout
Judge

Date: October 1, 2018

Cornell-Brown, Rowan

From: Haney, Rachel (Perkins Coie) <RHaney@perkinscoie.com>
Sent: Wednesday, October 3, 2018 5:33 PM
To: Kriger, Ryan; Engrav, Rebecca S. (Perkins Coie); Spear, Ryan M. (Perkins Coie)
Cc: 'Van Hise, Matthew'; Blackston, Elizabeth
Subject: RE: Docket No. 540-9-18 Wncv, State of Vermont vs. Uber Technologies, Inc., ORDER

Ryan,

Confirming receipt, thanks very much for sending.

Warm regards,

Rachel Haney | **Perkins Coie LLP**
ASSOCIATE
1201 Third Avenue Suite 4900
Seattle, WA 98101-3099
D. +1.206.359.8544
F. +1.206.359.9544
E. RHaney@perkinscoie.com

From: Kriger, Ryan [mailto:ryan.kriger@vermont.gov]
Sent: Wednesday, October 3, 2018 2:27 PM
To: Engrav, Rebecca S. (SEA) <REngrav@perkinscoie.com>; Haney, Rachel A.S. (SEA) <RHaney@perkinscoie.com>; Spear, Ryan M. (SEA) <RSpear@perkinscoie.com>
Cc: 'Van Hise, Matthew' <MVanHise@atg.state.il.us>; Blackston, Elizabeth <EBlackston@atg.state.il.us>
Subject: Fw: Docket No. 540-9-18 Wncv, State of Vermont vs. Uber Technologies, Inc., ORDER

Counsel,

Attached please find the signed Order in the Vermont Uber matter.

Thank you for all of your work on this.

-Ryan

Ryan G. Kriger
Assistant Attorney General
Vermont Office of the Attorney General
Public Protection Division
109 State Street
Montpelier, VT 05609-1001

ph: (802) 828-3170
ryan.kriger@vermont.gov

From: JUD - Washington Unit
Sent: Wednesday, October 3, 2018 4:31 PM
To: Kriger, Ryan
Cc: AGO - Consumer Info
Subject: Docket No. 540-9-18 Wncv, State of Vermont vs. Uber Technologies, Inc., ORDER

Please see the attached document: ORDER

Donna Waters

Washington Civil Division, Vermont Superior Court
65 State Street, Montpelier, Vermont 05602
Civil (802)828-2091^Small Claims (802)828-5551
www.vermontjudiciary.org

***** DO NOT REPLY ***** This email account is not monitored for responses. Please contact the court in person, by phone, or by U.S. mail if you need assistance.

***** CONFIDENTIAL ***** This email message and related attachments may contain personal and/or privileged information. If you are not the intended recipient, do not disseminate, distribute or copy this email message or any attachments. Please immediately notify JUD.Helpdesk@vermont.gov and permanently delete this email message and any attachments from your computer. For all other assistance, please contact the court.

EMAIL RECIPIENT INFORMATION:

RYAN G KRIGER (ryan.kriger@vermont.gov; ago.consumerinfo@vermont.gov)
Phone: (802)828-3170, ERN 4740

PERKINSCOIE

1201 Third Avenue
Suite 4900
Seattle, WA 98101-3099

+1.206.359.8000
+1.206.359.9000
PerkinsCoie.com

June 16, 2016

Amelia M. Gerlicher
AGerlicher@perkinscoie.com
D. +1.206.359.3445
F. +1.206.359.4445

VIA E-MAIL

Ryan Kriger, Assistant Attorney General
AJ Van Tassel, Investigator
Vermont Attorney General's Office
ago.securitybreach@state.vt.us

RE: Updated Information Regarding Previous Notification of Security Breach

Dear Mr. Kriger:

I write on behalf of Uber Technologies, Inc. ("Uber"), to update our February 26, 2015 notification regarding unauthorized access to electronic files in a proprietary database by a party unaffiliated with Uber. I specifically write to advise you that Uber has learned that the database contains the name and driver's license number of one additional resident of your state.

The database in question is highly complex from a technical standpoint. A forensic firm analyzing the database in connection with a lawsuit discovered additional information. As a result of this analysis, Uber learned that the database contains the driver's license numbers of additional drivers. We are sending the enclosed notification of the incident to all such individuals starting on June 16.

To date, Uber has not received any reports of actual misuse of any information as a result of this incident, including with respect to any of the individuals whose information was recently discovered in the database.

Please contact me at the above address with any questions or concerns regarding this incident.

Very truly yours,

Amelia M. Gerlicher

Enclosure

PO BOX 510390
LIVONIA MI 48151-6267
RETURN SERVICE REQUESTED

1455 Market Street
San Francisco, CA 94103
UBER.com

J04000

June 15, 2016

P19HVZ00100001-000687604

MOUSE1 MICKEY1
307 CALIFORNIA ST
SUISUN CITY CA 94585

RE: Notice of Data Breach. Please read this entire letter.

Dear **MOUSE1 MICKEY1** :

I'm writing to let you know that an Uber database was accessed by an unauthorized third party, and that as an Uber driver partner, your information may have been affected.

What Happened?
Uber discovered in September 2014 that information allowing access to the database had been available without intended access restrictions. We immediately ensured that the database was no longer accessible using that information, and have taken additional safety measures to protect your information. We also determined that the database was accessed only once by a third party, on May 13, 2014.

What Information Was involved?
Your name and driver's license number were contained in the database. Your information was not initially identified as part of the database; however, after extensive analysis and investigation, it was determined in May 2016 that your personal information was within the database. We have not received any reports of actual misuse of information as a result of this incident, but Uber recommends that you monitor your credit reports for fraudulent transactions or accounts.

What Are We Doing?
In addition to restricting access to the database as described above, Uber has continued to investigate the incident, resulting in this notice to you.

To help protect your identity, we are offering a complimentary one-year enrollment in My TransUnion Monitoring, a credit monitoring service provided by a subsidiary of TransUnion®, one of the three nationwide credit reporting agencies. This service helps detect possible misuse of your personal information, provides you with superior identity protection support focused on immediate identification and resolution of identity theft, and up to $1,000,000 in identity theft insurance with no deductible. More information on My TransUnion Monitoring is below.

What You Can Do
We recommend enrolling in the My TransUnion Monitoring service, and reviewing the additional steps described below.

If you have any questions about this incident, please contact us at notice@uber.com or call us at (800) 870-8534.

On behalf of Uber, I apologize for this inconvenience and thank you for your partnership.

Sincerely,

Legal Director - Privacy
Derek Care

Activate My TransUnion Monitoring in Three Easy Steps

To enroll in this service, go to **www.transunionmonitoring.com** and enter the following unique 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

You may alternatively enroll in a similar offline credit monitoring service that is delivered via U.S. Mail. To enroll, call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code **690137** and follow the additional steps provided to complete enrollment.

You can sign up for the online or offline credit monitoring service anytime between now and **September 30, 2016.** Enrolling in this service will not affect your credit score.

Additional Steps You Can Take

You may obtain a free copy of your credit report from each of the three credit reporting agencies by visiting www.annualcreditreport.com or by calling toll-free (877) 322-8228. Please review the reports carefully, and if you find anything you do not understand or that is incorrect, contact the appropriate credit-reporting agency for assistance. If you suspect fraud, you can also contact your local police, the attorney general of your state, or the Federal Trade Commission.

You may also contact the credit reporting agencies directly to put in place a fraud alert or a security freeze. A fraud alert will notify any merchant checking your credit history that you may be the victim of identity theft and that the merchant should verify the application. Contacting any one of the three agencies will place an alert on your file at all three. A security freeze restricts all creditor access to your account, but might also delay any requests you might make for new accounts. Ask the credit reporting agencies for their specific procedures regarding security freezes.

Equifax	**Experian**	**TransUnion**
1-800-525-6285	1-888-397-3742	1-800-680-7289
https://www.alerts.equifax.com	www.experian.com/fraud	www.transunion.com/fraud
https://www.freeze.equifax.com	www.experian.com/freeze	www.transunion.com/freeze
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19016-2000

The Federal Trade Commission also provides information about how to avoid identity theft and what to do if you suspect your identity has been stolen. They can be contacted at FTC Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, 1-877-ID-THEFT (877-438-4338) or consumer.ftc.gov.

Additional information for residents of North Carolina:
You can also contact your state attorney general for information on preventing identity theft: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com/, Telephone: 1-919-716-6400.

Additional information for residents of Maryland:
You can also contact your state attorney general for information on preventing identity theft: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

PERKINSCOIE

1201 Third Avenue
Suite 4900
Seattle, WA 98101-3099

+1.206.359.8000
+1.206.359.9000
PerkinsCoie.com

November 21, 2017

Rebecca S. Engrav
REngrav@perkinscoie.com
D. +1.206.359.6168
F. +1.206.359.7168

Ryan Kriger, Assistant Attorney General
AJ Van Tassel Sweet, Investigator
Consumer Protection Unit
Vermont Attorney General's Office
109 State Street
Montpelier, VT 05609-1001

Email Address: *ago.securitybreach@vermont.gov*

Re: Notification of Security Breach

To Whom It May Concern:

On behalf of our client Uber Technologies, Inc. ("Uber"), we are writing to notify you of a data security incident.

In November 2016, Uber was contacted by an individual who claimed he had accessed Uber user information. Uber investigated and determined that the individual and another person working with him had obtained access to certain stored copies of Uber databases and files located on Uber's private cloud data storage environment on Amazon Web Services. Uber determined the means of access, shut down a compromised credential, and took other steps intended to confirm that the actors had destroyed and would not use or further disseminate the information. Uber also implemented additional measures to improve its security posture. To the best of Uber's knowledge, the unauthorized actor's access to this data began on October 13, 2016, and there was no further access by the actor to Uber's data after November 15, 2016.

As determined by Uber and outside forensic experts, the accessed files contained user information that Uber used to operate the Uber service. Most of this information does not trigger data breach notifications under state law. However, the files did include, for a subset of users in the files, the names and driver's license numbers of about 600,000 Uber drivers in the United States, including at least 176 drivers in Vermont (we will update this number in the next few days after the mailing count is finalized).[1] Beginning on November 22, 2017, Uber is providing notice to the individuals whose driver's license information was downloaded in this incident. Uber will offer 12 months of credit monitoring and identity theft protection services to these individuals free of charge, and the notice will provide information on how to use such services. A copy of the notice is enclosed.

[1] The files also included other types of data and salted and hashed user passwords, but they do not trigger notification.

As it has publicly announced today, Uber now thinks it was wrong not to provide notice to affected users at the time. Accordingly, Uber is now providing notice. In order to treat its driver partners consistently throughout the United States, Uber is providing notice to affected drivers in all states without regard to whether the facts and circumstances of this incident (or the number of affected individuals) trigger notification in each particular state.

Uber is taking personnel actions with respect to some of those involved in the handling of the incident. In addition, Uber has implemented and will implement further technical security measures, including improvements related to both access controls and encryption.

Uber sincerely regrets that this incident occurred. It is committed to working with your office to address this matter. Please do not hesitate to contact me with any questions or for more information. My contact information is above.

Very truly yours,

Rebecca S. Engrav

Attachment

Return Mail Processing
P.O. Box 589
Claysburg, PA 16625-0589

1455 Market Street
San Francisco, CA 94103
UBER.com

##D2700-L01-0123456 0001 00000001 **********9-OELZZ 123
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

November 22, 2017

NOTICE OF DATA BREACH

Dear Sample A Sample:

I am writing to let you know about a data security incident at Uber that affected your information. Uber deeply regrets that this happened and we recommend that you closely review the information in this letter.

What Happened	In November 2016, Uber learned that unauthorized actors obtained access to a private cloud storage environment used by Uber. They accessed stored copies of Uber databases and files. To the best of our knowledge, the unauthorized access began on October 13, 2016 and ended no later than November 15, 2016.
What Information Was Involved	The accessed files contained user information that Uber used to operate the Uber service, including your name and driver's license number. The files included this information for about 600,000 Uber drivers in the United States.
What We Are Doing	We have made changes to our data storage environment and security procedures to decrease the chance of a similar occurrence in the future. To assist you, we are also providing identity theft protection and mitigation services from Experian, including credit monitoring, for twelve (12) months at no cost to you. See details below.
What You Can Do	We recommend enrolling in Experian IdentityWorks℠ and reviewing the additional information below.
For More Information	If you have any questions regarding this incident or if you desire further information or assistance, please contact (844) 439-7669.

Again, and on behalf of everyone at Uber, I am sorry that this happened. Drivers like you are at the heart of our service. Simply put, Uber wouldn't exist without you and we thank you for your partnership.

0123456

Sincerely,

Dara Khosrowshahi
Chief Executive Officer

Activate Experian IdentityWorks℠

We encourage you to activate the fraud detection tools available through Experian IdentityWorks℠ as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: February 28, 2018**. (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcreditone
- Provide your **activation code**: **ABCDEFGHI**

Additionally, complimentary Identity Restoration assistance is immediately available to you. If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one year from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

If you have questions about these products, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (844) 439-7669 by **February 28, 2018**. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Additional Steps You Can Take

Learn More and Report Suspected Identity Theft

You are encouraged to contact the Federal Trade Commission (FTC), law enforcement, or your state attorney general's office to report incidents of suspected identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.identitytheft.gov

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

You can contact the nationwide consumer reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

D2700-L01

You should remain vigilant for incidents of fraud, identity theft, and errors by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

Obtain Your Credit Reports

You should also monitor your credit reports. You may periodically obtain free credit reports from each nationwide consumer reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Place a Fraud Alert or Security Freeze on Your Credit Report File

A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. You should know that it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

A security freeze, sometimes called a credit freeze, is designed to prevent credit, loans, and services from being approved in your name without your consent. You should know that it also may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Unlike a fraud alert, you must separately place a security freeze on your credit file by sending a request to each of the three major credit reporting agencies listed above. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

With certain exceptions, a consumer reporting agency may charge you a fee to place a freeze on your credit report, to temporarily lift a freeze on your credit report, or to remove a freeze from your credit report.

IF YOU ARE A MARYLAND RESIDENT:
You may obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(410) 576-6491
www.oag.state.md.us

IF YOU ARE A NORTH CAROLINA RESIDENT:
You may obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.gov

IF YOU ARE A RHODE ISLAND RESIDENT:
You have the right to obtain a police report in regard to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Additionally, you may obtain information about preventing identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
http://www.riag.ri.gov/

IF YOU ARE A RESIDENT OF OTHER STATES:
Your state attorney general's office and website may also provide relevant information.