DAVID N. SONNENREICH, Bar No. 4917
Deputy Attorney General
SEAN D. REYES, Bar No. 7969
Utah Attorney General
PO Box 140872
160 East Broadway
Salt Lake City, Utah 84114-0872
Tel: (801) 366-0132
Fax: (801) 366-0315
Emails: dsonnenreich@agutah.gov
Attorneys for Plaintiff State of Utah

IN THE THIRD JUDICIAL DISTRICT COURT
STATE OF UTAH, SALT LAKE COUNTY

STATE OF UTAH Plaintiff, vs. UBER TECHNOLOGIES, INC. Defendant.	)	**FINAL JUDGMENT AND CONSENT DECREE** Civil No. 180907163 Judge Elizabeth A Hruby-Mills

Plaintiff, THE STATE OF UTAH, by Sean D. Reyes, Attorney General of the State of Utah, has filed a Complaint for a permanent injunction and other relief in this matter pursuant to the Utah Protection of Personal Information Act ("UPPIA"), Utah Code §§ 13-44-101, *et. seq.* and the Utah Consumer Sales Practices Act ("UCSPA"), Utah Code §§ 13-11-1, *et. seq.*, alleging Defendant, UBER TECHNOLOGIES, INC. ("UBER") committed violations of those acts.

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 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 UPPIA. The Utah Division of Consumer Protection is charged with enforcement of the UCSPA; the Attorney General acts as counsel to the Division.

---

[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.
[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.*

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 Utah, in that UBER is a technology company that provides a ride hailing mobile application that connects drivers with riders. Riders hail and pay drivers using the UBER platform.

Order

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

I. DEFINITIONS

1. "Covered Conduct" shall mean UBER's conduct related to the data breach involving UBER that occurred in 2016 and that UBER announced in 2017.
2. "Data Security Incident" shall mean any unauthorized access to Personal Information

owned, licensed, or maintained by UBER.

3. "Effective Date" shall be October 25, 2018.
4. "Encrypt," "Encrypted," or "Encryption" shall mean rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.
5. "Personal Information" shall have the definition as set forth in the UPPIA. Utah Code § 13-44-102(3).
6. "Riders and Drivers" or, as applicable, "Rider or Driver" shall mean any individual natural person who is a resident of Utah 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 Utah law. 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 UPPIA and UCSPA 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 UPPIA.
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 Utah 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.[5]

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 Utah, identifying and describing any Data Security

[5] Without limiting the availability of any other applicable protections from disclosure, this Final Judgment and Consent Decree shall be deemed to be a confidentiality order within the meaning of Utah Code § 13-44-301(7)(b).

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. Any payment made to the State of Utah will be allocated between the Attorney General's Office, and the Utah Division of Consumer Protection, Department of Commerce, and the National Attorneys General Training and Research Institute, as directed by counsel.

Release

20. Upon payment of the amount due to Utah under this Final Judgment and Consent Decree, the Attorney General shall release and discharge UBER from all civil claims that the Attorney General or the Utah Division of Consumer Protection could have brought under Utah Law or common law claims concerning unfair, deceptive, or fraudulent trade practices based on the Covered Conduct. Nothing contained in this paragraph shall be construed to limit the ability of the Attorney General to enforce the obligations that UBER has under this Final Judgment and Consent Decree. Further, nothing in this Final Judgment and Consent Decree shall be construed to create, waive, or limit any private right of action.

General Provisions

21. The parties understand and agree that this Final Judgment and Consent Decree shall not be construed as an approval or a sanction by the Attorney General of UBER's business practices, nor shall UBER represent that this Final Judgment and Consent Decree constitutes an approval or sanction of its business practices. The parties further understand and agree that any failure by the Attorney General to take any action in response to any information submitted pursuant to this Final Judgment and Consent Decree shall not be construed as an approval or sanction of any representations, acts, or practices indicated by such information, nor shall it preclude action thereon at a later date.
22. Nothing in this Final Judgment and Consent Decree shall be construed as relieving UBER of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of the provisions of this Final Judgment and Consent Decree be deemed to

be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

23. UBER shall deliver a copy of this Final Judgment and Consent Decree to, or otherwise fully apprise, its executive management having decision-making authority with respect to the subject matter of this Final Judgment and Consent Decree within thirty (30) days of the Effective Date.
24. To the extent that there are any, UBER agrees to pay all court costs associated with the filing (if legally required) of this Final Judgment and Consent Decree. No court costs, if any, shall be taxed against the Attorney General.
25. If any clause, provision, paragraph, or section of this Final Judgment and Consent Decree is for any reason held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, paragraph, or section of this Final Judgment and Consent Decree, and this Final Judgment and Consent Decree shall be construed and enforced as if such illegal, invalid, or unenforceable clause, provision, paragraph, or section had not been contained herein.
26. Any notice or report provided by UBER to the Attorney General under this Final Judgment and Consent Decree shall be satisfied by sending notice to the Designated Contacts in *Appendix B*. Any notice or report provided by the Attorney General to UBER under this Final Judgment and Consent Decree shall be satisfied by sending notice to: Chief Legal Officer, Uber Technologies, Inc., 1455 Market Street, San Francisco, California 94103; with a copy to Rebecca S. Engrav, Perkins Coie LLP, 1201 Third Avenue, Suite 4900, Seattle, Washington 98101. All such notices or reports shall be sent

by United States mail, certified mail return receipt requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the notice or document, and shall be deemed to be sent upon mailing. Notwithstanding the foregoing, if a sending party requests of the receiving party whether transmission by electronic mail is sufficient for a particular notice or report and the receiving party agrees, electronic mail may be used if an electronic return receipt is provided. An Attorney General may update its address by sending a complete, new updated version of *Appendix B* to UBER and to all other Attorneys General listed on *Appendix B*. UBER may update its address by sending written notice to all parties listed in *Appendix B*.

APPROVED:

PLAINTIFF, THE STATE OF UTAH

Attorney General Sean D. Reyes

By: ____/s/ David N. Sonnenreich_____ Date: __09-26-18_____

Deputy Attorney General David N. Sonnenreich

APPROVED:

DEFENDANT, UBER TECHNOLOGIES, INC.

By: _____/s/ Tony West_____ Date: _____09-21-18_____
Tony West
Chief Legal Officer

APPROVED:

COUNSEL FOR DEFENDANT, UBER TECHNOLOGIES, INC.

By: ____/s/ Barry G. Stratford_____ Date: _____09-21-18_____

Barry G. Stratford, Bar No. # 15059
Perkins Coie LLP
2901 N. Central Avenue, Suite 2000
Phoenix, Arizona 85012-2788
Telephone: (602) 351-8206
Facsimile: (602) 648-7035
Email: bstratford@perkinscoie.com
Local Counsel for Uber Technologies, Inc.

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

----------END OF FINAL JUDGEMENT AND CONSENT DECREE----------
*** ENTERED BY THE COURT ON THE DATE AND AS INDICATED BY THE COURT'S SEAL AT THE TOP OF THE FIRST PAGE ***

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