

IN THE MATTER OF: §  
TARGET CORPORATION §

**ASSURANCE OF VOLUNTARY COMPLIANCE**

This Assurance of Voluntary Compliance<sup>1</sup> is entered into by the Attorneys General of Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii<sup>2</sup>, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, 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, Vermont, Virginia, Washington and West Virginia, as well as the District of Columbia (referred to collectively as the “Attorneys General”) and Target Corporation to resolve the Attorneys General’s investigation into the security incident announced by Target on December 19, 2013 (collectively, the “Parties”).<sup>3</sup>

In consideration of their mutual agreements to the terms of this Assurance, and such other consideration as described herein, the sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

---

<sup>1</sup> This Assurance of Voluntary Compliance shall, for all necessary purposes, also be considered an Assurance of Discontinuance.

<sup>2</sup> Hawaii is represented on this matter by its Office of Consumer Protection, an agency which is not part of the state Attorney General’s Office, but which is statutorily authorized to undertake consumer protection functions, including legal representation of the State of Hawaii. For simplicity purposes, the entire group will be referred to as the “Attorneys General” or individually as “Attorney General” and the designations, as they pertain to Hawaii, refer to the Executive Director of the State of Hawaii’s Office of Consumer Protection.

<sup>3</sup> The State of California is simultaneously negotiating a settlement in a form consistent with the requirements of California law. That settlement would incorporate the substantive terms of this Assurance of Voluntary Compliance; to the extent there are differences, the differences will be related to and/or arise from the differences in the form. Payment to the State of California pursuant to its settlement with TARGET will be a portion of the total paid to the Attorneys General as recited in paragraph 29.

## **I. INTRODUCTION**

This Assurance constitutes a good faith settlement and release between TARGET and the Attorneys General of claims related to a data breach, publically announced by TARGET on December 19, 2013 and January 10, 2014, in which a person or persons gained unauthorized access to portions of TARGET's computer systems that process payment card transactions at TARGET's retail stores and to portions of TARGET's computer systems that store TARGET customer contact information (such intrusion referred to as the "Intrusion").

## **II. DEFINITIONS**

1. For the purposes of this Assurance, the following definitions shall apply:
  - A. "Cardholder Data Environment" shall mean TARGET's technologies that store, process, or transmit payment card authentication data, consistent with the Payment Card Industry Data Security Standard ("PCI DSS").
  - B. "Consumer" shall mean any individual who initiates a purchase of or purchases goods from a TARGET retail location; any individual who returns merchandise to a TARGET retail location; or any individual who otherwise provides Personal Information to TARGET in connection with any other retail transaction at a TARGET retail location.
  - C. "Consumer Protection Acts" shall mean the State citation(s) listed in Appendix A.
  - D. "Effective Date" shall be the date on which TARGET receives a copy of this Assurance duly executed in full by TARGET and by each of the Attorneys General.
  - E. "Personal Information" shall mean the following:

- i. For a Consumer that is a resident of a State that is a Party to this Assurance and that has a Consumer Protection Statute or Personal Information Protection Act, the data elements in the definitions of personal information as set forth in those Acts;
- ii. For a Consumer that is a resident of a State that is a Party to this Assurance and that does not have a Consumer Protection Statute or Personal Information Protection Act, the Consumer's first name or first initial and last name in combination with any one or more of the following data elements that relate to such individual: (a) Social Security number; (b) driver's license number; (c) state-issued identification card number; or (d) financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to the Consumer's financial account; and
- iii. For purposes of Paragraph 15, the first name or first initial and last name of a Consumer who is a resident of a State that is a Party to this Assurance in combination with any one or more of the following data elements that relate to such individual: (a) Social Security number; (b) driver's license number; (c) state-issued identification card number; or (d) financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to the Consumer's financial account.

- F. “Personal Information Protection Acts” shall mean the State citations listed in Appendix B.
- G. “Security Breach Notification Acts” shall mean the State citations listed in Appendix C.
- H. “TARGET” shall mean Target Corporation, its affiliates, subsidiaries and divisions, successors and assigns doing business in the United States.
- I. “Security Event” shall mean any potential compromise to the confidentiality, integrity, or availability of a TARGET information asset that includes Personal Information.

### **III. APPLICATION**

2. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance shall apply to TARGET, its affiliates, subsidiaries, successors and assigns, and its officers and employees.

### **IV. ASSURANCES**

3. TARGET shall comply with the Consumer Protection Statutes and the Personal Information Protection Acts in connection with its collection, maintenance, and safeguarding of Personal Information.

4. TARGET shall not misrepresent the extent to which TARGET maintains and protects the privacy, security, confidentiality, or integrity of any Personal Information collected from or about Consumers.

5. TARGET shall comply with the Security Breach Notification Acts. For any future breach of security involving the unauthorized access to or acquisition of Personal Information identified in Paragraph 1(E)(ii) and relating to a Consumer who is a resident of New

Mexico or South Dakota, TARGET shall provide notice to such Consumer and the New Mexico and/or South Dakota Attorney General's Office, as relevant, except that notice shall not be required if TARGET reasonably determines that there is not a reasonable likelihood that harm to the Consumer will result from the incident. To the extent that New Mexico or South Dakota enact a security breach notification law following the Effective Date, TARGET shall comply with such law in lieu of the requirement of the preceding sentence.

**A. INFORMATION SECURITY PROGRAM**

6. TARGET shall, within one hundred and eighty (180) days after the Effective Date of this Assurance, develop, implement, and maintain a comprehensive information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of Personal Information it collects or obtains from Consumers.

7. TARGET's Information Security Program shall be written and shall contain administrative, technical, and physical safeguards appropriate to:

- A. The size and complexity of TARGET's operations;
- B. The nature and scope of TARGET's activities; and
- C. The sensitivity of the Personal Information that TARGET maintains.

8. TARGET may satisfy the implementation and maintenance of the Information Security Program and the safeguards required by this Assurance through review, maintenance, and, if necessary, updating, of an existing information security program or existing safeguards, provided that such existing information security program and existing safeguards meet the requirements set forth herein.

9. TARGET shall employ an executive or officer with appropriate background or experience in information security who shall be responsible for implementing and maintaining the Information Security Program.

10. TARGET shall ensure that the role of the designated executive or officer, referenced in Paragraph 9, includes advising the Chief Executive Officer and the Board of Directors of TARGET's security posture, security risks faced by TARGET, and security implications of TARGET's decisions.

11. TARGET shall ensure that its Information Security Program receives the resources and support reasonably necessary to ensure that the Information Security Program functions as intended by this Assurance.

#### **B. ADMINISTRATIVE SAFEGUARDS**

12. TARGET shall develop, implement, and revise as necessary written, risk-based policies and procedures for auditing vendor compliance with TARGET's Information Security Program.

13. TARGET's Information Security Program shall be designed and implemented to ensure the appropriate handling and investigation of Security Events involving Personal Information.

14. TARGET shall make reasonable efforts to maintain and support the software on its networks, taking into consideration the impact an update will have on data security in the context of TARGET's overall network and its ongoing business and network operations, and the scope of the resources required to address an end-of-life software issue.

15. TARGET shall maintain encryption protocols and related policies that are reasonably designed to encrypt Personal Information identified in Paragraph 1(E)(iii) that

TARGET stores on desktops located within the Cardholder Data Environment, and shall encrypt the data elements of Personal Information identified in Paragraph 1(E)(iii), as well as any other data elements required by state law to be so encrypted, that are:

- A. Stored on laptops or other portable devices; or
- B. Transmitted wirelessly or across public networks.

16. TARGET shall comply with the Payment Card Industry Data Security Standard (“PCI DSS”) with respect to its Cardholder Data Environment, as defined in this Assurance, and any TARGET system component the compromise of which TARGET should reasonably believe would impact the security of the Cardholder Data Environment.

### **C. SPECIFIC SAFEGUARDS**

17. Segmentation:

- A. TARGET shall take reasonable, risk-based steps to scan and map the connections between its Cardholder Data Environment and the rest of its computer network in order to determine avenues of traffic to the Cardholder Data Environment and to identify and assess potential penetration vulnerabilities to the Cardholder Data Environment.
- B. TARGET’s Cardholder Data Environment shall be segmented from the rest of the TARGET computer network.
- C. TARGET shall develop and implement a risk-based penetration testing program reasonably designed to identify, assess, and remediate penetration vulnerabilities within TARGET’s computer network.

18. Access Control and Management:

- A. TARGET shall implement and maintain appropriate risk-based controls to manage access to, and use of, TARGET's individual accounts, TARGET's service accounts, and vendor accounts, including strong passwords and password-rotation policies.
- B. TARGET shall evaluate, and as appropriate, restrict and/or disable all unnecessary network programs that provide access to TARGET's Cardholder Data Environment and/or to any TARGET system component the compromise of which TARGET reasonably believes would also impact the security of the Cardholder Data Environment.
- C. TARGET shall adopt a reasonable and risk-based approach to integrate two-factor authentication into TARGET's individual accounts, TARGET's administrator accounts, and vendor accounts.

19. File Integrity Monitoring: TARGET shall deploy and maintain controls, including, but not limited to, a file integrity monitoring solution, designed to notify personnel of unauthorized modifications to critical applications or operating system files within the Cardholder Data Environment.

20. Whitelisting: TARGET shall deploy and maintain controls, such as, for example, an application whitelisting solution, designed to detect and/or prevent the execution of unauthorized applications within its point-of-sale terminals and in-store point-of-sale servers.

21. Logging and Monitoring:

- A. TARGET shall, to the extent technically feasible, implement reasonable controls to manage the access of any device attempting to connect to the Cardholder Data Environment, through hardware or software tools such as



firewalls, authentication credentials, or other such access restricting mechanisms.

- B. TARGET shall maintain an appropriate system to collect logs and monitor network activity, such as through the use of a security information and event management tool.

22. Change Control: TARGET shall develop and maintain policies and procedures with respect to managing and documenting changes to network systems.

23. Development: TARGET shall take steps reasonably designed to appropriately maintain the separation of development and production environments.

24. Payment Card Security: TARGET shall implement where appropriate steps designed to reasonably manage the review and, where reasonable and appropriate, the adoption of improved, industry-accepted payment card security technologies relevant to TARGET's business and Cardholder Data Environment, such as chip and PIN technology.

25. Devalue Payment Card Information: TARGET shall make reasonable efforts to devalue payment card information, including, but not limited to, encrypting payment card information throughout the course of a retail transaction at a TARGET retail location.

#### **V. SETTLEMENT COMPLIANCE ASSESSMENT**

26. TARGET shall obtain an information security assessment and report from a third-party professional ("Third-Party Assessor"), using procedures and standards generally accepted in the profession ("Third-Party Assessment"), within one (1) year after the Effective Date of this Assurance. The Third-Party Assessor's report on the Third-Party Assessment shall:

- A. Set forth the specific administrative, technical, and physical safeguards maintained by TARGET;

- B. Explain the extent to which such safeguards are appropriate in light of TARGET's size and complexity, the nature and scope of TARGET's activities, and the sensitivity of the Personal Information maintained by TARGET;
- C. Explain the extent to which the safeguards that have been implemented meet the requirements of the Information Security Program; and
- D. Identify TARGET's Qualified Security Assessor for purposes of PCI DSS compliance.

27. TARGET's Third-Party Assessor shall be: (a) a Certified Information Systems Security Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or a similarly qualified person or organization; and (b) have at least five (5) years of experience evaluating the effectiveness of computer systems or information system security.

#### **VI. SUBMISSION TO ATTORNEYS GENERAL**

28. TARGET shall provide a copy of the Third-Party Assessor's report on the Third-Party Assessment to the Connecticut Attorney General's Office within one hundred and eighty (180) days of the completion of the report.

- A. Confidentiality: The Connecticut Attorney General's Office shall treat the Third-Party Assessment report as exempt from disclosure under the relevant public records laws, pursuant to this Assurance or, as necessary, by employing other means to ensure confidentiality.
- B. State Access to Report: The Connecticut Attorney General's Office may provide a copy of the report on Third-Party Assessment received from TARGET to any other of the Attorneys General upon request, and each

requesting Attorney General shall, to the extent permitted by the laws of the Attorney General's State, treat such report as exempt from disclosure under the relevant public records laws.

#### **VII. PAYMENT TO THE STATES**

29. TARGET shall pay Eighteen Million Five Hundred Thousand Dollars (\$18,500,000) to the Attorneys General. Said payment shall be divided and paid by TARGET directly to each of the Attorneys General in an amount designated by the Attorneys General and communicated to TARGET by the Illinois Attorney General and Connecticut Attorney General. Each of the Attorneys General agrees that the Illinois Attorney General and Connecticut Attorney General have the authority to designate such amount to be paid by TARGET to each Attorney General and to provide TARGET with instructions for the payments to be distributed under this Paragraph. Payment shall be made no later than thirty (30) days after the Effective Date of this Assurance and receipt of such payment instructions by TARGET from the Illinois Attorney General and Connecticut Attorney General, except that where state law requires judicial or other approval of the Assurance, payment shall be made no later than thirty (30) days after notice from the relevant Attorney General that such final approval for the Assurance has been secured.

30. Said payment shall be used by the Attorneys General for such purposes that may include, but are not limited to, attorneys' fees and other costs of investigation, or to be placed in, or applied to, the 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 costs of the inquiry leading hereto, or for other uses permitted by state law, at the sole discretion of the Attorneys General.

## **VIII. RELEASE AND EXPIRATION**

31. Following full payment of the amounts due under this Assurance, the Attorneys General shall release and discharge TARGET from all civil claims that the Attorneys General could have brought under the Consumer Protection Acts, the Personal Information Protection Acts, and the Security Breach Notification Acts based on TARGET's conduct related to the Intrusion. Nothing contained in this paragraph shall be construed to limit the ability of the Attorneys General to enforce the obligations that TARGET has under this Assurance. Further, nothing in this Assurance shall be construed to create, waive, or limit any private right of action.

32. The obligations and other provisions of this Assurance set forth in paragraphs 9, 10, 15, 16, 17.A., 17.B., 18, 19, 20, and 23 shall expire at the conclusion of the five (5) year period after the Effective Date of this Assurance, unless they have expired at an earlier date pursuant to their specific terms. Provided, however, that nothing in this paragraph should be construed or applied to excuse TARGET from its obligation to comply with all applicable state and federal laws, regulations, and rules.

## **IX. MEET AND CONFER**

33. If any Attorney General determines that TARGET has failed to comply with any of the terms of this Assurance, and if in the Attorney General's sole discretion the failure to comply does not threaten the health or safety of the citizens of the Attorney General's State and/or does not create an emergency requiring immediate action, the Attorney General will notify TARGET in writing of such failure to comply and TARGET shall have thirty (30) days from receipt of such written notice to provide a good faith written response to the Attorney General's determination. The response shall include: (A) a statement explaining why TARGET believes it is in full compliance with this Assurance; or (B) a detailed explanation of how the

alleged violation(s) occurred, and (i) a statement that the alleged violation has been addressed and how, or (ii) a statement that the alleged violation cannot be reasonably addressed within thirty (30) days from receipt of the notice, but (a) TARGET has begun to take corrective action(s) to address the alleged violation, (b) TARGET is pursuing such corrective action(s) with reasonable diligence, and (c) TARGET has provided the Attorney General with a reasonable timetable for addressing the alleged violation.

34. Nothing herein shall prevent an Attorney General from agreeing in writing to provide TARGET with additional time beyond the thirty (30) day period to respond to the notice provided under Paragraph 33.

35. Nothing herein shall be construed to exonerate any failure to comply with any provision of this Assurance after the Effective Date, or to compromise the authority of an Attorney General to initiate a proceeding for any failure to comply with this Assurance.

#### **X. PRESERVATION OF AUTHORITY**

36. Nothing in this Assurance shall be construed to limit the authority or ability of an Attorney General to protect the interests of his/her State or the people of his/her State. This Assurance shall not bar the Attorney General or any other governmental entity from enforcing laws, regulations, or rules against TARGET for conduct subsequent to or otherwise not covered by this Assurance. Further, nothing in this Assurance shall be construed to limit the ability of the Attorney General to enforce the obligations that TARGET has under this Assurance.

#### **XI. GENERAL PROVISIONS**

37. The Parties understand and agree that this Assurance shall not be construed as an approval or a sanction by the Attorneys General of TARGET's business practices, nor shall TARGET represent that this Assurance constitutes an approval or sanction of its business

practices. The Parties further understand and agree that any failure by the Attorneys General to take any action in response to any information submitted pursuant to this Assurance 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.

38. Nothing in this Assurance shall be construed as relieving TARGET of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of the provisions of this Assurance be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

39. TARGET shall deliver a copy of this Assurance to, or otherwise fully apprise, its Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, the executive or officer of Paragraph 9, and General Counsel, and its Board of Directors within ninety (90) days of the Effective Date. TARGET shall deliver a copy of this Assurance to, or otherwise fully apprise, any new Chief Executive Officer, new Chief Information Officer, new Chief Information Security Officer, new executive or officer of Paragraph 9, and new General Counsel, and each new member of its Board of Directors, within ninety (90) days from which such person assumes his/her position with TARGET.

40. To the extent that there are any, TARGET agrees to pay all court costs associated with the filing (if legally required) of this Assurance. No court costs, if any, shall be taxed against any Attorney General.

41. TARGET shall not participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited by this Assurance or for any other purpose that would otherwise circumvent any term of this

Assurance. TARGET shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Assurance.

42. This Assurance may be executed by any number of counterparts and by different signatories on separate counterparts, each of which shall constitute an original counterpart thereof and all of which together shall constitute one and the same document. One or more counterparts of this Assurance may be delivered by facsimile or electronic transmission with the intent that it or they shall constitute an original counterpart thereof.

43. TARGET agrees that this Assurance does not entitle it to seek or to obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and TARGET further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

44. This Assurance shall not be construed to waive any claims of sovereign immunity the States may have in any action or proceeding.

## **XII. SEVERABILITY**

45. If any clause, provision, or section of this Assurance shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity or unenforceability shall not affect any other clause, provision or section of this Assurance and this Assurance shall be construed and enforced as if such illegal, invalid or unenforceable clause, section or provision had not been contained herein.

## **XIII. NOTICE/DELIVERY OF DOCUMENTS**

46. Whenever TARGET shall provide notice to the Attorneys General under this Assurance, that requirement shall be satisfied by sending notice to the Designated Contacts on behalf of the Attorneys General listed in Appendix D. Any notices or other documents sent to TARGET pursuant to this Assurance shall be sent to the following address: (1) Target

Corporation, ATTN: General Counsel, 1000 Nicollet Mall, Minneapolis, MN 55403; and (2) Nathan Taylor, Morrison & Foerster LLP, 2000 Pennsylvania Ave., NW, Suite 6000, Washington DC 20006. All notices or other documents to be provided under this Assurance 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 have been deemed to be sent upon mailing. Any party may update its address by sending written notice to the other party.



In the Matter of:  
Target Corporation  
Assurance of Voluntary Compliance

**OHIO**

MIKE DeWINE  
Attorney General of the State of Ohio



Michael S. Ziegler  
Principal Assistant Attorney General  
Office of the Ohio Attorney General  
Consumer Protection Section  
30 East Broad Street, 14th Floor  
Columbus, Ohio 43215

Date: May 8, 2017

**TARGET CORPORATION**

By:  \_\_\_\_\_  
Carter Leuty  
Vice President, Law  
TARGET CORPORATION

Date: May 15, 2017

## Appendix A.

STATE	CONSUMER PROTECTION ACTS
Alaska	Alaska Unfair Trade Practices and Consumer Protection Act, AS 45.50. 471 et seq.
Arizona	Arizona Consumer Fraud Act, A.R.S. §§ 44-1521 – 44-1534
Arkansas	Deceptive Trade Practices Act, Ark. Code Ann. § 4-88-101 et seq.
Colorado	Colorado Consumer Protection Act, C.R.S. § 6-1-101 et seq.
Connecticut	Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110a, et seq.
District of Columbia	Consumer Protection Procedures Act, D.C. Code, § 28-3901, et seq.
Delaware	Consumer Fraud Act, 6 Del.C. § 2511, et al.; Uniform Deceptive Trade Practices Act, 6 Del.C. § 2531, et al.
Florida	Florida Deceptive and Unfair Trade Practices Act, § 501.201 et seq., Fla. Stat.
Georgia	Fair Business Practices Act, O.C.G.A. § 10-1-390 through 408
Hawaii	Uniform Deceptive Trade Practice Act- Haw. Rev. Stat. Chpt. 481A and Haw. Rev. Stat. Sect. 480-2
Idaho	Idaho Consumer Protection Act, title 48, chapter 6, Idaho Code
Illinois	Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 <i>et seq.</i>
Indiana	Deceptive Consumer Sales Act; Indiana Code chapter 24-5-0.5
Iowa	Iowa Consumer Fraud Act, Iowa Code § 714.16
Kansas	Kansas Consumer Protection Act K.S.A 50-623 et al.
Kentucky	Kentucky Consumer Protection Act, Ky. Rev. Stat. 367.110-.300
Louisiana	Unfair Trade Practices and Consumer Protection Law, LA. Rev. Stat. 51:1401, et seq.
Maine	Maine Unfair Trade Practices Act, 5 M.R.S. § 205-A et seq.
Maryland	Maryland Consumer Protection Act, Md. Code Ann., Com. Law § 13-101, et seq. (2013 Repl. Vol and 2016 Supp.)
Massachusetts	Massachusetts Consumer Protection Act

## Appendix A.

	(Mass. Gen. Laws ch. 93A)
Michigan	Michigan Consumer Protection Act, Mich. Comp. Laws §§ 445.901, <i>et seq.</i>
Minnesota	Minnesota Deceptive Trade Practices Act, Minn. Stat. §§ 325D.43-.48; and Minnesota Prevention of Consumer Fraud Act, Minn Stat. § 325F.68-.69 and .70
Mississippi	Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1 <i>et seq.</i>
Missouri	Missouri Merchandising Practices Act, Chapter 407, RSMo.
Montana	Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. § 30-14-101 <i>et seq.</i>
Nebraska	Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1601 <i>et seq.</i> , and Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301 <i>et seq.</i>
Nevada	Nevada Deceptive Trade Practices Act; Nev. Rev. Stat. §§ 598.0903-598.0999
New Hampshire	NH RSA 358-A
New Jersey	New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 <i>et seq.</i>
New Mexico	Unfair Practices Act (UPA) NMSA 1978 Section 57-12-1 <i>et seq</i>
New York	Executive Law 63(12), General Business Law 349 and 350
North Carolina	North Carolina Unfair and Deceptive trade Practices Act, N.C. Gen. Stat. §§ 75-1.1, <i>et seq.</i>
North Dakota	N.D.C.C. ch. 51-15 (§51-15-02); Unlawful Sales or Advertising Practices
Ohio	Consumer Sales Practices Act, R.C. 1345.01 <i>et seq.</i>
Oklahoma	Oklahoma Consumer Protection Act, 15 O.S. §§ 751 <i>et seq.</i>
Oregon	Unlawful Trade Practices Act, ORS 646.605 <i>et seq.</i>
Pennsylvania	Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1, <i>et seq.</i>
Rhode Island	Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1, <i>et seq.</i>
South Carolina	South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-10, <i>et seq.</i>
South Dakota	South Dakota Codified Laws (SDCL)

## Appendix A.

	Chapter 37-24
Tennessee	Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. §§ 47-18-101 et seq.
Texas	Texas Deceptive Trade Practices Act, Tex. Bus. & Com. Code Ann. § 17.41 (West 2011)
Utah	Utah Consumer Sales Practices Act, Utah Code § 13-11-1 et seq.
Vermont	Vermont Consumer Protection Act, 9 V.S.A. § 2453
Virginia	Virginia Consumer Protection Act, Virginia Code §§ 59.1-196 through 59.1-207
Washington	Consumer Protection Act, RCW 19.86.020
West Virginia	West Virginia Consumer Credit and Protection Act (“WVCCPA”), W. Va. Code § 46A-1-101, et al.

## Appendix B.

STATE	PERSONAL INFORMATION PROTECTION ACTS
Alaska	Alaska Personal Information Protection Act, AS 45.48.010 et seq.
Arkansas	Personal Information Protection Act, Ark. Code Ann. § 4-110-101 et seq.
Colorado	Colorado Consumer Protection Act, C.R.S. § 6-1-101 et sec.; Notification of Security Breach, C.R.S. § 6-1-716
Connecticut	Safeguarding of Personal Information, Conn. Gen. Stat. § 42-471
Florida	Florida Information Protection Act, § 501.171, Fla. Stat.
Georgia	Georgia Personal Identity Protection Act, O.C.G.A § 10-1-910 through 915
Hawaii	Personal Information Protection – Haw. Rev. Stat. Chpt. 487J
Illinois	Illinois Personal Information Protection Act, 815 ILCS 530/1 et seq.
Indiana	Disclosure of Security Breach Act; Indiana Code section 24-4.9-3-3.5
Kansas	Wayne Owen Act K.S.A. 50-6,139b
Maryland	Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3501, et seq. (2013 Repl. Vol and 2016 Supp.)
Massachusetts	Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth (201 C.M.R. 17.00 et seq.)
Minnesota	Minnesota Use of Social Security Numbers Statute, Minn. Stat. § 325E.59; and Minnesota Access Devices Statute, Minn. Stat. § 325E.64
Missouri	Missouri Merchandising Practices Act, Section 407.1500.1(9)
Montana	Impediment of Identity Theft Act, Mont. Code Ann. § 30-14-1701 et seq.
Nevada	Nevada Security of Personal Information Act; Nev. Rev. Stat. §§ 603A.010, et seq.
North Carolina	North Carolina Identity Theft Protection Act, N.C. Gen. Stat. §§ 75-60, et seq.
North Dakota	N.D.C.C. ch. 51-13: Notice of Security Breach for Personal Information
Oregon	Oregon Consumer Identity Theft Protection Act, ORS 646A.600 et seq.
Rhode Island	Rhode Island Identity Theft Protection Act, R.I. Gen. Laws § 11-49.3-1, et seq.

## Appendix B.

South Carolina	The Family Privacy Protection Act, S.C. Code Ann. § 30-2-10, <i>et seq.</i>
Texas	<u>Texas Identify Theft Enforcement and Protection Act, Tex. Bus. &amp; Com. Code Ann. Ch. 521 (West 2015)</u>
Utah	Protection of Personal Information Act, Utah Code § 13-44-101 <i>et seq.</i>
West Virginia	W. Va. Code § 46A-2A-101, <i>et al.</i>

## Appendix C.

STATE	SECURITY BREACH NOTIFICATION ACTS
Alaska	Alaska Breach of Security Involving Personal Information statutes, AS 45.48.010-45.48.090
Arizona	Notification of Breach of Security System, A.R.S. § 18-545
Arkansas	Disclosure of Security Breaches, Ark. Code Ann. § 4-110-105
Colorado	Colorado Consumer Protection Act; Notification of Security Breach § 6-1-716
Connecticut	Breach of Security re Computerized Data Containing Personal Information, Conn. Gen. Stat. § 36a-701b
District of Columbia	Security Notification Act, D.C. Code § 28-3851, <i>et seq.</i>
Delaware	6 <i>Del.C.</i> § 12B-101, <i>et al.</i>
Florida	Florida Information Protection Act, § 501.171, Fla. Stat.
Georgia	Georgia Personal Identity Protection Act, O.C.G.A. § 10-1-910 through 915
Hawaii	Security Breach of Personal Information- Haw. Rev. Stat. Chpt. 487N
Illinois	Illinois Personal Information Protection Act, 815 ILCS 530/1 <i>et seq.</i>
Indiana	Disclosure of Security Breach Act; Indiana Code article 24-4.9
Iowa	Iowa Personal Information Security Breach Protection Act, Iowa Code § 715C
Kansas	K.S.A 50-7a01 <i>et al.</i>
Kentucky	Ky. Rev. Stat. 365.732
Louisiana	Database Security Breach Notification Law, La. Rev. Stat. 51:3071, <i>et seq.</i> , and Reporting Requirements, La. Admin. Code tit. 16, pt. 3, §701.
Maine	Maine Notice of Risk to Personal Data Act, 10 M.R.S. § 1346, <i>et seq.</i>
Maryland	Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3501, <i>et seq.</i> (2013 Repl. Vol and 2016 Supp.)
Massachusetts	Massachusetts Security Breach Law (Mass. Gen. Laws ch. 93H)
Michigan	Identity Theft Protection Act, Mich. Comp. Laws §§ 445.61, <i>et seq.</i>
Minnesota	Minnesota Data Breach Notification Statute, Minn. Stat. § 325E.61
Mississippi	Notice of Breach of Security, Miss. Code Ann. §

## Appendix C.

	75-24-29
Missouri	Missouri Merchandising Practices Act, Section 407.1500, RSMo.
Montana	Impediment of Identity Theft Act, Mont. Code Ann. § 30-14-1704.
Nebraska	Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. § 87-801 et seq.
Nevada	Nev. Rev. Stat. § 603A.220 (located within the Nevada Security of Personal Information Act)
New Hampshire	NH RSA 359-C: 19-21
New Jersey	New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166
New York	The New York State Information Security Breach and Notification Act (General Business Law 899-aa)
North Carolina	North Carolina Identity Theft Protection Act, Protection from security breaches, N.C. Gen. Stat. § 75-65
North Dakota	N.D.C.C. ch. 51-13: Notice of Security Breach for Personal Information
Ohio	“Private disclosure of security breach of computerized personal information data”, R.C. 1349.19 et seq.
Oklahoma	Security Breach Notification Act, 24 O.S. §§ 161 et seq.
Oregon	Oregon Consumer Identity Theft Protection Act, ORS 646A.600 et seq.
Pennsylvania	Breach of Personal Information Notification Act, 73 P.S. §§ 2301, et seq.
Rhode Island	Rhode Island Identity Theft Protection Act, R.I. Gen. Laws § 11-49.3-4
South Carolina	The South Carolina Identity Fraud and Identity Theft Protection Act, S.C. Code Ann. § 1-11-490, et seq.
Tennessee	Tenn. Code Ann. § 47-18-2107 (this statute is within the Tennessee Identity Theft Deterrence Act of 1999, Tenn. Code Ann. §§ 47-18-2101 et seq.)
Texas	<u>Texas Identify Theft Enforcement and Protection Act, Tex. Bus. &amp; Com. Code Ann. Ch. 521(West 2015)</u>
Utah	Protection of Personal Information Act, Utah Code § 13-44-101 et seq.
Vermont	Vermont Security Breach Notice Act, 9 V.S.A. § 2435



## Appendix C.

Virginia	Virginia Code § 18.2-186.6
Washington	Data Breach Notification Law, RCW 19.255.010
West Virginia	WVCCPA, Breach of Security of Consumer Information, W. Va. Code § 46A-2A-101, et al.

## Appendix D.

STATE	ATTORNEYS GENERAL DESIGNATED CONTACTS
Alaska	<p>Davyn Williams  Assistant Attorney General  Alaska Office of the Attorney General  1031 W. 4<sup>th</sup> Ave, Suite 200  Anchorage, AK 99501  davyn.williams@alaska.gov  (907) 375-7778</p>
Arizona	<p>Taren Ellis Langford  Unit Chief Counsel  Arizona Attorney General's Office  400 W. Congress Street, Suite S-315  Tucson, AZ 85701  Taren.Langford@azag.gov  (520) 628-6631</p>
Arkansas	<p>Peggy Johnson  Assistant Attorney General  Office of the Arkansas Attorney General  323 Center Street, Suite 500  Little Rock, Arkansas 72201  peggy.johnson@arkansasag.gov  (501) 682-8062</p>
Colorado	<p>Jay Simonson  First Assistant Attorney General  Colorado Attorney General's Office  1300 Broadway 7<sup>th</sup> Fl.  Denver CO 80203  jay.simonson@coag.gov  (720) 508-6205</p>
Connecticut	<p>Matthew F. Fitzsimmons  Assistant Attorney General  Department Head  Privacy and Data Security Department  Office of the Attorney General  110 Sherman Street  Hartford CT 06105  Matthew.Fitzsimmons@ct.gov  (860) 808-5515</p>
District of Columbia	<p>Philip Ziperman  Director, Office of Consumer Protection  Office of the District of Columbia Attorney General  441 – 4<sup>th</sup> Street, N.W., 6<sup>th</sup> Floor  Washington, DC 20001  philip.ziperman@dc.gov  (202) 442-9886</p>

## Appendix D.

Delaware	<p>Stephen McDonald  Deputy Attorney General  Delaware Department of Justice  820 N. French St., 5<sup>th</sup> Floor  Wilmington, DE 19801  Stephen.McDonald@state.de.us  (302) 577-8513</p>
Florida	<p>Patrice Malloy  Chief, Multi-State and Privacy Bureau  Sr. Assistant Attorney General  Office of the Attorney General  110 S.E. 6<sup>th</sup> Street  Fort Lauderdale, FL 33301  Patrice.Malloy@myfloridalegal.com  (954) 712-4669</p>
Georgia	<p>Daniel S. Walsh  Senior Assistant Attorney General  Department of Law  State of Georgia  40 Capitol Square, SW  Atlanta, Georgia 30334-1300  dwalsh@law.ga.gov  (404) 657-2204</p>
Hawaii	<p>Lisa P. Tong  Enforcement Attorney  State of Hawaii Office of Consumer Protection  235 S. Beretania Street #801  Honolulu, Hawaii 96813  ltong@dcca.hawaii.gov  (808) 586-5978</p>
Idaho	<p>Stephanie Guyon  Deputy Attorney General  Idaho Attorney General's Office  Consumer Protection Division  954 W. Jefferson Street, 2<sup>nd</sup> FL.  Boise, ID 83702  stephanie.guyon@ag.idaho.gov  (208) 334-4135</p>
Illinois	<p>Matthew W. Van Hise, CIPP/US  Assistant Attorney General  Consumer Privacy Counsel  Consumer Fraud Bureau  Illinois Attorney General's Office  500 South Second Street  Springfield, IL 62706  mvanhise@atg.state.il.us  (217) 782-9024</p>

## Appendix D.

Indiana	Ernâni Magalhães Deputy Attorney General Consumer Protection Division Office of Attorney General Curtis Hill 302 West Washington Street IGCS-5th Floor Indianapolis, IN 46204 ernani.magalhaes@atg.in.gov (317) 234-6681
Iowa	Nathan Blake Assistant Attorney General Office of the Attorney General of Iowa 1305 E. Walnut St. Des Moines, IA 50319 nathan.blake@iowa.gov (515) 281-4325
Kansas	Sarah M. Dietz Assistant Attorney General Office of Kansas Attorney General Derek Schmidt 120 SW 10 <sup>th</sup> Avenue, 2 <sup>nd</sup> Floor sarah.dietz@ag.ks.gov (785) 296-3751
Kentucky	Kevin R. Winstead Assistant Attorney General Kentucky Attorney General's Office of Consumer Protection 1024 Capital Center Dr., #200 Frankfort, KY 40601 kevin.winstead@ky.gov (502) 696-5379
Louisiana	L. Christopher Styron Section Chief - Consumer Protection Assistant Attorney General Louisiana Department of Justice 1885 N. Third Street Baton Rouge, Louisiana 70802 styronl@ag.louisiana.gov (225) 326-6468
Maine	Christina Moylan Assistant Attorney General Maine Office of the Attorney General Cross State Office Building, 6 <sup>th</sup> Floor 109 Sewall St. 6 State House Station Augusta, Maine 04333-0006 christina.moylan@maine.gov (207) 626-8838

## Appendix D.

Maryland	Richard Trumka Jr. Assistant Attorney General Consumer Protection Division Office of the Attorney General 200 St. Paul Pl. Baltimore, MD 21202 rtrumka@oag.state.md.us (410) 576-6957
Massachusetts	Sara Cable Director, Data Privacy & Security Assistant Attorney General Consumer Protection Division Office of Attorney General Maura Healey Commonwealth of Massachusetts One Ashburton Place Boston MA 02108 sara.cable@state.ma.us (617) 963-2827
Michigan	Mark Gabrielse Assistant Attorney General Michigan Department of Attorney General Corporate Oversight Division P.O. Box 30755 Lansing, MI 48909 gabrielsem@michigan.gov (517) 373-1160
Minnesota	David Cullen Assistant Attorney General Minnesota Attorney General's Office 445 Minnesota Street, Suite 1400 St. Paul, MN 55101 David.Cullen@ag.state.mn.us (651) 757-1221
Mississippi	Crystal Utley Secoy Special Assistant Attorney General Consumer Protection Division Mississippi Attorney General's Office Post Office Box 22947 Jackson, Mississippi 39225 cutle@ago.state.ms.us (601) 359-4213

## Appendix D.

Missouri	Joyce Yeager Assistant Attorney General Consumer Protection Section Office of the Missouri Attorney General PO Box 899 Jefferson City, MO 65102 joyce.yeager@ago.mo.gov (573) 751-6733
Montana	Kelley L. Hubbard Assistant Attorney General Montana Office of Consumer Protection 555 Fuller Ave Helena, MT 59601 khubbard@mt.gov (406) 444-5790
Nebraska	Daniel Birdsall Assistant Attorney General Consumer Protection Division Nebraska Attorney General's Office 2115 State Capitol Building Lincoln, NE 68509 dan.birdsall@nebraska.gov (402) 471-3840
Nevada	Lucas J. Tucker Senior Deputy Attorney General Office of the Nevada Attorney General Bureau of Consumer Protection 10791 W. Twain Ave., Suite #100 Las Vegas, NV 89135 ltucker@ag.nv.gov (702) 486-3256
New Hampshire	James T. Boffetti Senior Assistant Attorney General Chief, Consumer Protection and Antitrust Bureau Department of Justice 33 Capitol Street Concord, New Hampshire 03301 James.Boffetti@doj.nh.gov (603) 271-0302

## Appendix D.

New Jersey	Elliott M. Siebers Deputy Attorney General Affirmative Civil Enforcement Practice Group Office of the Attorney General State of New Jersey 124 Halsey St. – 5 <sup>th</sup> Floor P.O. Box 45029-5029 Newark, NJ 07101 Elliott.Siebers@dol.lps.state.nj.us (973) 648-4460
New Mexico	Elizabeth K. Korsmo Assistant Attorney General Consumer and Environmental Protection Division New Mexico Office of the Attorney General 408 Galisteo St. Santa Fe, NM 87504 ekorsmo@nmag.gov (505) 660-7593
New York	Clark Russell Deputy Bureau Chief Bureau of Internet and Technology New York State Office of the Attorney General 120 Broadway New York, NY 10271-0332 clark.russell@ag.ny.gov (212) 416-6494
North Carolina	Kim D'Arruda, CIPP/US Special Deputy Attorney General North Carolina Department of Justice Consumer Protection Division 114 West Edenton Street Raleigh, NC 27603 kdarruda@ncdoj.gov (919) 716-6013
North Dakota	Brian M. Card Assistant Attorney General Consumer Protection & Antitrust Division Office of Attorney General of North Dakota 1050 E. Interstate Ave., Suite 200 Bismarck, ND 58503-5574 bmc card@nd.gov (701) 328-5570

## Appendix D.

Ohio	Michael Ziegler Principal Assistant Attorney General Office of the Ohio Attorney General - Consumer Protection Section 30 East Broad Street, 14th Floor Columbus, Ohio 43215 michael.ziegler@ohioattorneygeneral.gov (614) 466-3980
Oklahoma	Rachel Irwin Assistant Attorney General Consumer Protection Unit Oklahoma Attorney General's Office 313 NE 21 <sup>st</sup> Street Oklahoma City, OK 73105 Rachel.Irwin@oag.ok.gov (405) 522-1014
Oregon	Eva Novick Assistant Attorney General Financial Fraud/Consumer Protection Section Oregon Department of Justice 100 SW Market Street Portland, OR 97201 eva.h.novick@doj.state.or.us (971) 673-1880
Pennsylvania	Nicole R. DiTomo Deputy Attorney General Pennsylvania Office of Attorney General Bureau of Consumer Protection 15th Floor, Strawberry Square Harrisburg, PA 17120 nditomo@attorneygeneral.gov (717) 705-6559
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



## Appendix D.

South Carolina	Chantelle L. Neese Assistant Attorney General SC Attorney General's Office Consumer Protection & Antitrust Section Rembert C. Dennis Bldg 1000 Assembly St. P. O. Box 11549 Columbia, SC 29211 CNeese@scag.gov (803) 734-2346
South Dakota	Philip D. Carlson Assistant Attorney General Consumer Protection Division South Dakota Attorney General 1302 E. Hwy. 14, Ste. 1 Pierre, SD 57501 Phil.Carlson@state.sd.us (605) 773-3216
Tennessee	Carolyn Smith Senior Counsel Consumer Protection and Advocate Division 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 Attorney General Consumer Protection Division P.O. Box 12548 Austin, Texas 78711 Esther.Chavez@oag.texas.gov (512) 475-4628
Utah	David N. Sonnenreich Deputy Attorney General Office of the Utah Attorney General 160 East 300 South, 5th Floor P.O. Box 140872 dsonnenreich@agutah.gov (801) 366-0132

## Appendix D.

Vermont	Ryan Kriger Assistant Attorney General Vermont Office of the Attorney General Public Protection Division 109 State St. Montpelier, VT 05609 ryan.kriger@vermont.gov (802) 828-3170
Virginia	Stephen John Sovinsky Assistant Attorney General Office of the Attorney General 202 North Ninth Street Richmond, Virginia 23219 ssovinsky@oag.state.va.us (804) 823-6341
Washington	Andrea Alegrett Assistant Attorney General Consumer Protection Division Office of the Washington Attorney General 800 Fifth Avenue, Suite 2000 Seattle, WA 98104 andreaa1@atg.wa.gov (206) 389-3813
West Virginia	Laurel K. Lackey Assistant Attorney General Office of the Attorney General Eastern Panhandle Office 269 Aikens Center Martinsburg, WV 25404 laurel.k.lackey@wvago.gov (304) 267-0239