

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET AND TECHNOLOGY

In the Matter of

Assurance No. 17-094

**Investigation by ERIC T. SCHNEIDERMAN,
Attorney General of the State of New York, of**

TARGET CORPORATION,

Respondent.

ASSURANCE OF VOLUNTARY COMPLIANCE

This Assurance of Voluntary Compliance¹ is entered into by the Attorneys General of Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii², 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

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

² 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.

(collectively, the "Parties").³

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:

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

³ 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.

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.

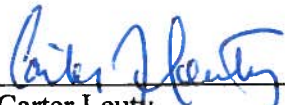
XIII. NOTICE/DELIVERY OF DOCUMENTS

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.

**ERIC T. SCHNEIDERMAN
NEW YORK ATTORNEY GENERAL**

TARGET CORPORATION

By: 
Clark Russell
Deputy Bureau Chief, Bureau of Internet and Technology
Office of the New York State Attorney General
120 Broadway
New York, NY 10271-0332
Phone: (212) 416-8433
Fax: (212) 416-8369

By: 
Carter Leuty
Vice President, Law
TARGET CORPORATION

May 8, 2017
Date

May 15, 2017
Date