SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SAN FRANCISCO

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, **v.** **TARGET CORPORATION, a corporation,** Defendant.	Case No. CGC-17-559105 **FINAL JUDGMENT AND PERMANENT INJUNCTION**

Plaintiff, the People of the State of California, appearing through its attorney, Xavier Becerra, Attorney General of the State of California, by Yen P. Nguyen, Deputy Attorney General, (hereinafter collectively "the People" or "Plaintiff"), and Defendant Target Corporation, a corporation (hereinafter referred to as "Target" or "Defendant"), appearing through its attorney, Nathan D. Taylor of Morrison & Foerster LLP, having stipulated to the entry of this Final Judgment and Permanent Injunction ("Judgment") by the Court without the taking of proof and without trial or adjudication of any fact or law, without this Judgment constituting evidence of or an admission by Target regarding any issue of law or fact alleged in the Complaint on file, and without Target admitting any liability, and with all parties having waived their right to appeal, and the Court having considered the matter and good cause appearing:

IT IS HEREBY ORDERED, ADJUDGED, AND DECREED THAT:

I. PARTIES AND JURISDICTION

1. The People of the State of California is the Plaintiff in this case.

2. Target Corporation is the Defendant in this case.

3. The Court has jurisdiction over the subject matter of this action, jurisdiction over the parties to this action, and venue is proper in this Court.

4. Defendant, at all relevant times, has transacted business in the State of California, including, but not limited to, San Francisco County.

5. This Judgment is entered pursuant to and subject to California Business and Professions Code section 17200 et seq.

II. DEFINITIONS

6. For the purposes of this Judgment, 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. "Unfair Competition Law" shall mean California Business and Professions Code section 17200 et seq.

d. "Effective Date" shall be the date on which this Judgment is entered by the Court.

e. "Personal Information" shall mean the following:

i. The data elements in the definition of personal information as set forth in the Reasonable Data Security Law;

ii. For purposes of Paragraph 8.m, the first name or first initial and last name of a Consumer residing in California 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. "Reasonable Data Security Law" shall mean California Civil Code section 1798.81.5.

g. "Data Breach Notification Law" shall mean California Civil Code section 1798.82.

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.

j. "Intrusion" shall mean 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.

III. PERMANENT INJUNCTIVE RELIEF

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

8. In accordance with section 17203 of the California Business and Professions Code, Defendant shall comply with the following conduct requirements:

a. TARGET shall comply with the Unfair Competition Law and the Reasonable Data Security Law in connection with its collection, maintenance, and safeguarding of Personal Information.

b. 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.

c. TARGET shall comply with the Data Breach Notification Law.

Information Security Program

d. TARGET shall, within one hundred and eighty (180) days after the Effective Date of this Judgment, 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.

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

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

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

iii. The sensitivity of the Personal Information that TARGET maintains.

f. TARGET may satisfy the implementation and maintenance of the Information Security Program and the safeguards required by this Judgment 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.

g. 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.

h. TARGET shall ensure that the role of the designated executive or officer, referenced in Paragraph 8.g, 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.

i. 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 Judgment.

Administrative Safeguards

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

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

l. 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.

m. TARGET shall maintain encryption protocols and related policies that are reasonably designed to encrypt Personal Information identified in Paragraph 6.e.ii that TARGET stores on desktops located within the Cardholder Data Environment, and shall encrypt the data elements of Personal Information identified in Paragraph 6.e.ii, as well as any other data elements required by state law to be so encrypted, that are:

i. Stored on laptops or other portable devices; or

ii. Transmitted wirelessly or across public networks.

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

Specific Safeguards

o. Segmentation:

i. 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.

ii. TARGET's Cardholder Data Environment shall be segmented from the rest of the TARGET computer network.

iii. 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.

p. Access Control and Management:

i. 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.

ii. 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.

iii. 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.

q. 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.

r. 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.

s. Logging and Monitoring:

i. 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.

ii. 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.

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

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

v. 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.

w. 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.

IV. SETTLEMENT COMPLIANCE ASSESSMENT

9. 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 Judgment. 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.

10. 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.

V. SUBMISSION TO THE ATTORNEY GENERAL

11. 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. 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 the California Attorney General upon request, and the California Attorney General shall, to the extent permitted by the laws of the State of California, treat such report as exempt from disclosure under the relevant public records laws.

VI. MONETARY PAYMENT

12. As memorialized in the Assurances of Voluntary Compliance ("AVC") with the Attorneys General of other states resolving similar allegations, TARGET shall pay a total of Eighteen Million Five Hundred Thousand Dollars ($18,500,000) to the states, a portion of which Defendant shall pay within thirty (30) days of the Effective Date of this Judgment to the California Attorney General in the amount communicated to Defendant by the Illinois Attorney General and Connecticut Attorney General.

13. Said payment shall be used to defray the costs of the investigation leading to this Judgment, and for the California Attorney General's enforcement of consumer protection laws, at the sole discretion of the California Attorney General.

VII. RELEASE AND EXPIRATION

14. Following full payment of the amount due under this Judgment, the California Attorney General shall release and discharge TARGET from all civil claims that the California Attorney General could have brought under the Unfair Competition Law, the Reasonable Data Security Law, and the Data Breach Notification Law based on TARGET's conduct related to the Intrusion. Nothing contained in this paragraph shall be construed to limit the ability of the California Attorney General to enforce the obligations that TARGET has under this Judgment. Further, nothing in this Judgment shall be construed to create, waive, or limit any private right of action.

15. The obligations and other provisions of this Judgment set forth in paragraphs 8.g, 8.h, 8.m, 8.n, 8.o.i, 8.o.ii, 8.p, 8.q, 8.r, and 8.u shall expire at the conclusion of the five (5) year period after the Effective Date of this Judgment, 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.

VIII. GENERAL PROVISIONS

16. If the California Attorney General determines that TARGET has failed to comply with any of the terms of this Judgment, and if in the California Attorney General's sole discretion the failure to comply does not threaten the health or safety of the citizens of California and/or does not create an emergency requiring immediate action, the California 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 California Attorney General's determination. The response shall include: (A) a statement explaining why TARGET believes it is in full compliance with this Judgment; 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 California Attorney General with a reasonable timetable for addressing the alleged violation.

17. 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 16.

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

19. Nothing in this Judgment shall be construed to limit the authority or ability of the California Attorney General to protect the interests of California or the people of California. This Judgment shall not bar the California 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 Judgment. Further, nothing in this Judgment shall be construed to limit the ability of the California Attorney General to enforce the obligations that TARGET has under this Judgment.

20. Nothing in this Judgment 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 Judgment be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

21. TARGET shall deliver a copy of this Judgment to, or otherwise fully apprise, its Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, the executive or officer of Paragraph 8.g, and General Counsel, and its Board of Directors within ninety (90) days of the Effective Date. TARGET shall deliver a copy of this Judgment 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 8.g, 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.

22. TARGET shall pay all court costs associated with the filing of this Judgment.

23. 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 Judgment or for any other purpose that would otherwise circumvent any term of this Judgment. TARGET shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Judgment.

24. TARGET agrees that this Judgment 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.

25. This Judgment shall not be construed to waive any claims of sovereign immunity California may have in any action or proceeding.

26. If any clause, provision, or section of this Judgment 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 Judgment and this Judgment shall be construed and enforced as if such illegal, invalid or unenforceable clause, section or provision had not been contained herein.

27. Whenever TARGET shall provide notice to the California Attorney General under this Judgment, that requirement shall be satisfied by sending notice: Yen P. (TiTi) Nguyen, Deputy Attorney General, Office of the Attorney General, 455 Golden Gate Avenue, Suite 11000, San Francisco, CA 94102-7004. Any notices or other documents sent to TARGET pursuant to this Judgment 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 Judgment 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

28. Jurisdiction is retained by the Court for the purpose of enabling any party to the Judgment to apply to the Court at any time for such further orders and directions as may be necessary or appropriate for the construction or the carrying out of this Judgment, for the modification of any of the injunctive provisions hereof, for enforcement of compliance herewith, and for the punishment of violations hereof, if any.

29. The clerk is ordered to enter this Judgment forthwith.

ORDERED AND ADJUDGED at San Francisco, California, this 23 day of May, 2017.

HAROLD KAHN

Judge of the Superior Court