STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

STATE OF VERMONT,

Plaintiff,

v.

BOEHRINGER INGELHEIM PHARMACEUTICALS, INC.,

Defendant.

CIVIL DIVISION
Docket No. 729-12-17 Wncv

FINAL CONSENT JUDGMENT

Plaintiff the State of Vermont has filed a Complaint for a permanent injunction and other relief in this matter pursuant to 9 V.S.A. § 2451, *et seq.* of the Vermont Consumer Protection Act ("CPA"), and Plaintiff, by its counsel, and Defendant Boehringer Ingelheim Pharmaceuticals, Inc. (BIPI), by its counsel, have agreed to the entry of this Final Consent Judgment by the Court without trial or adjudication of any issue of fact or law, and without finding or admission of wrongdoing or liability of any kind of any violation of the CPA as alleged by Plaintiff.

IT IS HEREBY ORDERED THAT:

1. PARTIES

1.1 Plaintiff, the State of Vermont is charged with the enforcement of the CPA.

1.2 Defendant, Boehringer Ingelheim Pharmaceuticals, Inc., is a Delaware corporation with its principal place of business at 900 Ridgebury Road in Ridgefield,

Connecticut. At all relevant times, BIPI did business in Vermont by marketing, selling, and Promoting the drugs Aggrenox, Atrovent, Combivent, and Micardis (hereinafter the "Covered Products").

2. PREAMBLE

2.1 BIPI represents it voluntarily established a compliance program that is applicable to all BIPI employees prior to the execution of this Judgment.

2.2 BIPI further represents its compliance program includes a Compliance Officer; a Code of Conduct; written policies and procedures; education and training initiatives; a disclosure program that allows for confidential disclosure and investigation of potential compliance violations and appropriate disciplinary procedures; and regular internal auditing procedures.

3. FINDINGS

3.1 This Court has jurisdiction over the subject matter of this lawsuit and over all parties.

3.2 The terms of this Judgment shall be governed by the laws of the State of Vermont.

3.3 Entry of this Judgment is in the public interest and reflects a negotiated agreement among the parties.

3.4 The parties have agreed to resolve the issues resulting from the Covered Conduct by entering into this Judgment.

3.5 BIPI is willing to enter into this Judgment regarding the Covered Conduct in order to resolve the Signatory Attorney General's concerns under the State Consumer Protection Laws as to the matters addressed in this Judgment and thereby avoid significant expense, inconvenience, and uncertainty.

3.6 BIPI is entering into this Judgment solely for the purpose of settlement, and nothing contained herein may be taken as or construed to be an admission or concession of any

violation of law, or regulation, or of any other matter of fact or law, or of any liability or wrongdoing, including allegations in the Complaint, all of which BIPI expressly denies. BIPI does not admit any violation of law, and does not admit any wrongdoing that was or could have been alleged by the Signatory Attorney General before the date of the Judgment. No part of this Judgment, including its statements and commitments, shall constitute evidence of any liability, fault, or wrongdoing by BIPI.

3.7 This Judgment shall not be construed or used as a waiver or limitation of any defense otherwise available to BIPI in any action, or of BIPI's right to defend itself from, or make any arguments in, any private individual, regulatory, governmental, or class claims or suits relating to the subject matter or terms of this Judgment. Nothing in this Judgment shall waive, release, or otherwise affect any claims, defenses, or positions BIPI may have in connection with any investigations, claims, or other matters the State/Commonwealth is not releasing hereunder. This Judgment is made without trial or adjudication of any issue of fact or law or finding of liability of any kind. It is the intent of the parties that this Judgment shall not be binding or admissible in any other matter, including, but not limited to, any investigation or litigation, other than in connection with the enforcement of this Judgment. Unless otherwise provided under state law, no part of this Judgment shall create a private cause of action or confer any right to any third party for violation of any federal or state statute except that a State may file an action to enforce the terms of this Judgment. Notwithstanding the foregoing, the State of Vermont may file an action to enforce the terms of this Judgment.

3.8 This Judgment (or any portion thereof) shall in no way be construed to prohibit, limit, or restrict BIPI from making representations with respect to the Covered Products that are permitted or authorized under federal law, the Federal Food, Drug & Cosmetic Act ("FDCA"),

21 U.S.C. § 301 et seq., U.S. Food and Drug Administration ("FDA") regulations, or FDA Guidances for Industry, currently issued or as revised. Further, the Judgment shall in no way prohibit, limit, or restrict BIPI from making representations with respect to the Covered Products that are required or authorized by, or consistent with the FDA-approved Labeling or prescribing information, or by any Investigational New Drug Application, New Drug Application, Supplemental New Drug Application, or Abbreviated New Drug Application filed with the FDA so long as the representation, taken in its entirety, is not false, misleading or deceptive.

3.9 Nothing in this Judgment shall require BIPI to:

(a) take any action that is prohibited by the Food, Drug and Cosmetic Act, 21 U.S.C. § 301 *et seq.* ("FDCA") or any regulation promulgated thereunder, or by the FDA; or

(b) fail to take any action that is required by the FDCA or any regulation promulgated thereunder, or by the FDA.

4. DEFINITIONS

The following definitions shall be used in construing this Judgment:

4.1 "BIPI" means Boehringer Ingelheim Pharmaceuticals, Inc., including all of its past and present subsidiaries, predecessors, successors, and assigns.

4.2 "BIPI Marketing" shall mean BIPI personnel responsible for marketing Covered Products in the United States.

4.3 "BIPI Medical" shall mean BIPI personnel who are highly trained experts with specialized scientific or medical knowledge whose roles involve the provision of specialized medical or scientific information, scientific analysis, and/or scientific information to HCPs but excludes anyone performing sales, marketing, or other commercial roles.

4.4 "BIPI Sales" shall mean the BIPI sales force responsible for sales of Covered Products in the United States, including, but not limited to, the field force and all management personnel such as district managers, regional managers, vice president(s) over sales, and president over sales.

4.5 "Clear(ly) and Conspicuous(ly)" shall mean, with respect to a disclosure or information presented, that such information meets requirements of the FDCA, the requirements of FDA regulations, and the recommended actions in FDA Guidances for Industry, including FDA's "Guidance for Industry: Presenting Risk Information in Prescription Drug and Medical Device Promotion," or as revised.

4.6 "Covered Conduct" shall mean BIPI's Promotional and marketing practices, and dissemination of information and remuneration to HCPs regarding the Covered Products through the Effective Date of the Judgment.

4.7 "Covered Product" shall mean BIPI drugs: Aggrenox, Atrovent, Combivent, and Micardis, which have all been approved by FDA.

4.8 "Effective Date" shall mean the date on which a copy of this Judgment, duly executed by BIPI and by the Signatory Attorney General, is approved by, and becomes a Judgment of the Court.

4.9 "FDA Guidances for Industry" shall mean documents, as currently drafted or as revised, issued by the FDA pursuant to 21 U.S.C. §371(h) that represent the FDA's current thinking on a topic.

4.10 "HCP" shall mean any physician or other health care practitioner, who is licensed to provide health care services or to prescribe pharmaceutical products.

4.11 "Labeling" shall mean all labels and other written, printed, or graphic matter (a) upon any article or any of its containers or wrappers, or (b) accompanying such article.

4.12 "Medical Information Response(s)" shall mean a non-Promotional, scientific communication to address an Unsolicited Request for medical information from a HCP.

4.13 "Multistate Executive Committee" shall mean the Attorneys General and their staffs representing Arizona, the District of Columbia, Illinois, Indiana, Kansas, Nevada, Pennsylvania, Tennessee, and Texas.

4.14 "Multistate Working Group" shall mean the Attorneys General and their staffs representing Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, the District of Columbia, Florida, Georgia, Hawaii[1], 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[2], Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

4.15 "Off-Label" shall mean a use, including indication, dosage, population, and/or method of administration, not consistent with the use approved by the FDA in the Labeling for a Covered Product at the time information regarding such use was communicated, or at the time the conduct occurred.

---

[1] Hawaii is being 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, the entire group will be referred to as the "Attorneys General," and such designation, as it includes Hawaii, refers to the Executive Director of the State of Hawaii Office of Consumer Protection.

[2] The Utah Attorney General's Office represents the Utah Division of Consumer Protection (Division), the state agency charged with enforcement of the Consumer Sales Practices Act, in this action, but is not a party itself. As to Utah, the definition of "Attorneys General" means the Utah Attorney General as counsel to the Division.

4.16 "Promotional," "Promoting," or "Promote" shall mean representations made to HCPs, patients, consumers, payors, and other customers, about a Covered Product and other practices intended to increase sales in the United States or that attempt to influence prescribing practices of HCPs in the United States, including direct-to-consumer.

4.17 "Promotional Materials" shall mean any item used to Promote a Covered Product.

4.18 "Promotional Speaker(s)" shall mean a HCP speaker engaged by or on behalf of BIPI to Promote a Covered Product in the United States.

4.19 "Reprints Containing Off-Label Information" shall mean articles or reprints from a scientific or medical journal, as defined in 21 C.F.R. 99.3(j), or reference publication, as defined in 21 C.F.R. 99.3(i), describing an Off-Label use of a Covered Product.

4.20 "Signatory Attorney General" shall mean the Attorney General of Vermont, or his authorized designee, who has agreed to this Judgment.

4.21 "State Consumer Protection Laws" shall mean the CPA.

4.22 "Unsolicited Request" shall mean a request for information communicated to an agent of BIPI that has not been prompted by or on behalf of BIPI.

4.23 Any reference to a written document shall mean a physical paper copy of the document, an electronic version of the document, or electronic access to such document.

5. COMPLIANCE PROVISIONS

The following Compliance Provisions, Paragraphs 5.3 through 5.24, shall apply for five (5) years from the Effective Date of this Judgment.

Promotional Activities

5.1 BIPI shall not make, or cause to be made, any written or oral claim that is false, misleading, or deceptive regarding any Covered Product.

5.2 BIPI shall not represent that any Covered Product has any sponsorship, approval, characteristics, ingredients, uses, benefits, quantities, or qualities that it does not have.

5.3 BIPI shall not promote any Covered Product for any Off-Label use.

5.4 In Promotional Materials for Covered Products, BIPI shall Clearly and Conspicuously disclose the risks associated with the Covered Products as set forth in the products' Labeling and shall present information about effectiveness and risk in a balanced manner.

5.5 BIPI shall require that all Promotional Speakers for any Covered Product comply with BIPI's obligations contained in this Judgment.

5.6 BIPI shall notify BIPI Sales promptly of any warning letter received from the FDA that affects the conduct of any sales representative in Promoting the relevant Covered Product and shall promptly disseminate a description of the concerns described in the warning letter.

5.7 BIPI shall not Promote a Covered Product by misrepresenting any clinical treatment guideline in a manner that suggests a Covered Product is approved for uses not consistent with the FDA-approved prescribing information.

Product Sampling

5.8 BIPI shall provide samples of a Covered Product only to those HCPs whose clinical practice is consistent with the product's FDA-approved Labeling.

5.9 If a HCP whose clinical practice is inconsistent with a Covered Product's Labeling requests samples of that Covered Product, BIPI personnel shall refer the HCP to BIPI Medical where the HCP can speak directly with a BIPI Medical representative who will provide answers to the HCP's questions about the Covered Product, and BIPI may provide him/her with samples only if appropriate (i.e., if the HCP requests the samples for an FDA-approved [on-label] use).

Financial Incentives to BIPI Sales and/or BIPI Marketing

5.10 BIPI's financial incentives shall be designed to ensure that BIPI Sales and/or BIPI Marketing are not motivated to engage in improper Promotion, sales, and marketing of Covered Products.

5.11 BIPI's financial incentives shall not include mechanisms to provide incentive compensation for sales that may indicate Off-Label use of any Covered Product.

Dissemination and Exchange of Medical Information

5.12 The content of BIPI's communications concerning Off-Label uses of a Covered Product shall not be false, misleading, or deceptive. BIPI shall not knowingly disseminate any Medical Information Response, including one that describes any Off-Label use of a Covered Product, unless such information and materials comply with the standards in applicable FDA regulations and with recommendations in FDA Guidances for Industry.

5.13 BIPI Sales and BIPI Marketing shall not develop Medical Information Responses regarding a Covered Product.

5.14 Medical Information Responses to Unsolicited Requests for Off-Label information regarding a Covered Product may be disseminated only by BIPI Medical, except in circumstances implicating public health or safety issues.

5.15 BIPI Medical shall have ultimate responsibility for developing and approving all Medical Information Responses regarding a Covered Product. Additional approvals may be provided by BIPI's legal department. BIPI shall not distribute any such materials unless:

(a) clinically relevant information is included in these materials to provide scientific balance;

(b) data in these materials are presented in an unbiased, non-Promotional manner; and

(c) these materials are Clearly and Conspicuously distinguishable from sales aids and other Promotional Materials.

5.16 Nothing in this subsection shall prohibit BIPI Medical from disseminating materials that are permitted to be distributed under Federal law, Federal regulations, or FDA published Guidance, unless false, misleading, or deceptive.

Responses to Unsolicited Requests for Off-Label Information

5.17 If BIPI elects to respond to an Unsolicited Request for Off-Label information regarding a Covered Product, BIPI Medical shall provide specific, accurate, objective, and scientifically balanced responses. Any such response shall not Promote a Covered Product for any Off-Label use.

5.18 Any written BIPI response to an Unsolicited Request for Off-Label information regarding a Covered Product shall be a Medical Information Response and shall include:

(a) a copy of the FDA-required Labeling, if any, for the Covered Product (e.g., FDA-approved package insert and, if the response is for a consumer, FDA-approved patient Labeling);

(b) a prominent statement notifying the recipient that the FDA has not approved or cleared the Covered Product as safe and effective for the Off-Label use addressed in the accompanying materials;

(c) a prominent statement disclosing the uses for which FDA has approved or cleared the Covered Product; and

(d) a report containing the results of a reasonable literature search using terms from the request.

5.19 BIPI Sales and BIPI Marketing may respond orally to an Unsolicited Request for Off-Label information regarding a Covered Product only by offering to refer the request to BIPI Medical or by offering to put the HCP in touch with BIPI Medical.

Reprints Containing Off-Label Information

5.20 BIPI shall not disseminate information describing any Off-Label or unapproved use of a Covered Product, unless such information and materials comply with the standards in applicable FDA regulations and with recommendations in FDA Guidances for Industry, including FDA's "Guidance for Industry: Responding to Unsolicited Requests for Off-Label Information About Prescription Drugs and Medical Devices" and FDA's "Guidance for Industry: Distributing Scientific and Medical Publications on Unapproved New Uses – Recommended Practices," or as revised.

5.21 BIPI Medical shall be responsible for the identification, selection, approval and dissemination of Reprints Containing Off-Label Information regarding a Covered Product.

5.22 Reprints Containing Off-Label Information regarding a Covered Product:

(a) shall be accompanied by the FDA approved Labeling for the Covered Product or a prominently displayed and Clearly and Conspicuously described hyperlink that

will provide the reader with such information;

(b) shall contain a Clear and Conspicuous disclosure in a prominent location, which would include the first page or as a cover page where practicable, indicating that the article discusses Off-Label information; and

(c) shall not be referred to or used in a Promotional manner.

5.23 Reprints Containing Off-Label Information regarding a Covered Product may only be disseminated if approved by BIPI Medical to HCPs.

5.24 This section of the Judgment does not apply to reprints containing only incidental references to Off-Label information. If reprints have an incidental reference to Off-Label information, such reprints shall contain the disclosures required by Paragraph 5.22 (a) and Paragraph 5.22 (b) in a prominent location, as defined above, and such incidental reference to Off-Label information shall not be referred to or used in a Promotional manner as prohibited by Paragraph 5.22 (c).

6. PAYMENT

6.1 No later than 30 days after the Effective Date of this Judgment, BIPI shall pay a total amount of Thirteen Million Five Hundred Thousand Dollars ($13,500,000) to be divided and paid by BIPI directly to each Signatory Attorney General of the Multistate Working Group in an amount to be designated by and in the sole discretion of the Multistate Executive Committee. Of that amount, Vermont shall receive one hundred thirty thousand, eight hundred sixty dollars and forty-one cents ($130, 860.41). Said payment shall be used by the States as attorneys' fees and other costs of investigation and litigation, or to be placed in, or applied to, the consumer protection enforcement fund, including future consumer protection enforcement, consumer education, litigation or local consumer aid fund or revolving fund, used to defray the costs of the inquiry leading hereto, or any lawful purpose, at the sole discretion of each Signatory

Attorney General, and in Vermont, pursuant to the Constitution of the State of Vermont, Ch. II § 27 and 32 V.S.A. § 462. The parties acknowledge that the payment described herein is not a fine, penalty, or payment in lieu thereof.

7. RELEASE

7.1 By its execution of this Judgment, the State of Vermont releases BIPI and all of its past and present subsidiaries, predecessors, successors, assigns, parents, affiliates, each of their current and former officers, directors, shareholders, employees, agents, contractors, and attorneys (collectively, the Released Parties) from the following: all civil claims, *parens patriae* claims, causes of action, damages, restitution, fines, attorney's fees, costs, and penalties that the Vermont Attorney General has asserted or could have asserted against the Released Parties under the above-cited consumer protection statutes or any common law claims concerning unfair, fraudulent, or deceptive trade practices other than those described in Paragraph 7.2 resulting from the Covered Conduct up to and including the Effective Date.

7.2 Notwithstanding any term of this Judgment, specifically reserved and excluded from the release in Paragraph 7.1 as to any entity or person, including Released Parties, are any and all of the following:

(a) any criminal liability that any person and/or entity, including Released Parties, has or may have to the State of Vermont;

(b) any civil or administrative liability that any person and/or entity, including Released Parties, has or may have to the State of Vermont not expressly covered by the release in Paragraph 7.1 above, including, but not limited to, any and all of the following claims:

(i) state or federal antitrust violations;

(ii) claims involving "best price," "average wholesale price," "wholesale acquisition cost," or any price-reporting practices;

(iii) Medicaid claims, including, but not limited to, federal Medicaid drug rebate statute violations, Medicaid fraud or abuse, and/or kickback violations related to any State's Medicaid program;

(iv) state false claims violations; and

(v) actions of state program payors of the State of Vermont arising from the purchase of a Covered Product, except for the release of civil penalties under 9 V.S.A. § 2451, et seq. of the CPA.

(c) any claims individual consumers have or may have under the CPA, and any common law claims individual consumers may have concerning unfair, fraudulent or deceptive trade practices, against any person and/or entity, including Released Parties.

8. DISPUTE RESOLUTION

8.1 For the purposes of resolving disputes with respect to compliance with this Judgment, should any of the Signatory Attorneys General have a reasonable basis to believe that BIPI has engaged in a practice that violates a provision of this Judgment subsequent to the Effective Date of this Judgment, then such Attorney General shall notify BIPI in writing of the specific objection, identify with particularity the provision of this Judgment that the practice appears to violate, and give BIPI 30 days to respond to the notification; provided, however, that a Signatory Attorney General may take any action if the Signatory Attorney General concludes that, because of the specific practice, a threat to the health or safety of the public requires immediate action. Upon receipt of written notice, BIPI shall provide a good-faith written response to the Attorney General notification, containing either a statement explaining why BIPI

believes it is in compliance with the Judgment, or a detailed explanation of how the alleged violation occurred and a statement explaining how BIPI intends to remedy the alleged breach. Nothing in this section shall be interpreted to limit the state's Civil Investigative Demand ("CID") or investigative subpoena authority, to the extent such authority exists under applicable law, and BIPI reserves all of its rights in responding to a CID or investigative subpoena issued pursuant to such authority.

8.2 Upon giving BIPI 30 days to respond to the notification described above, the Signatory Attorney General shall also be permitted reasonable access to inspect and copy relevant, non-privileged, non-work product records and documents in the possession, custody, or control of BIPI that relate to BIPI's compliance with each provision of this Judgment pursuant to that State's CID or investigative subpoena authority. If the Signatory Attorney General makes or requests copies of any documents during the course of that inspection, the Signatory Attorney General will provide a list of those documents to BIPI.

8.3 The Signatory Attorney General may assert any claim that BIPI has violated this Judgment in a separate civil action to enforce compliance with this Judgment, or may seek any other relief afforded by law, but only after providing BIPI an opportunity to respond to the notification described in Paragraph 8.1 above; provided, however, that the Signatory Attorney General may take any action if the Signatory Attorney General concludes that, because of the specific practice, a threat to the health or safety of the public requires immediate action.

9. GENERAL PROVISIONS

9.1 BIPI shall not cause third parties, acting on its behalf, to engage in practices from which BIPI is prohibited by this Judgment.

9.2 This Judgment does not constitute an approval by any of the Signatory Attorneys General of BIPI's business practices, and BIPI shall make no representation or claim to the

contrary.

9.3 Any failure by any party to this Judgment to insist upon the strict performance by any other party of any of the provisions of this Judgment shall not be deemed a waiver of any of the provisions of this Judgment, and such party, notwithstanding such failure, shall have the right thereafter to insist upon the specific performance of any and all of the provisions of this Judgment. This Judgment represents the full and complete terms of the settlement entered into by the parties hereto. In any action undertaken by the parties, no prior versions of this Judgment or any of its terms that were not entered by the Court in this Judgment, may be introduced for any purpose whatsoever.

9.4 This Court retains jurisdiction of this Judgment and the parties hereto for the purpose of enforcing and modifying this Judgment and for the purpose of granting such additional relief as may be necessary and appropriate.

9.5 This Judgment may be executed in counterparts, and a facsimile or .pdf signature shall be deemed to be, and shall have the same force and effect as, an original signature.

9.6 To the extent that any provision of this Judgment obligates BIPI to change any policy(ies) or procedure(s) and to the extent not already accomplished, BIPI shall implement the policy(ies) or procedure(s) as soon as reasonably practicable, but no later than 90 days after the Effective Date of this Judgment.

9.7 The parties agree that neither of them shall be deemed the drafter of this Judgment and that, in construing this Judgment, no provision hereof shall be construed in favor of one party on the ground that such provision was drafted by the other.

9.8 All notices under this Judgment shall be provided to the following via email and Overnight Mail:

For the State of Vermont:
Jill S. Abrams
Vermont Attorney General's Office
109 State Street
Montpelier, VT 05609

For Boehringer Ingelheim Pharmaceuticals, Inc.:

Wick Sollers
King & Spalding LLP
1700 Pennsylvania Avenue, N.W.
Washington, DC 20006
wsollers@kslaw.com

IT IS SO ORDERED, ADJUDGED AND DECREED.

December 26, 2017
Date

Mary Miles Teachout
Presiding Judge
Mary Miles Teachout

JOINTLY APPROVED AND
SUBMITTED FOR ENTRY

FOR PLAINTIFF, STATE OF VERMONT
THOMAS J. DONOVAN, JR.

Date: Dec. 20, 2017

Jill S. Abrams
Vermont Attorney General's Office
109 State Street
Montpelier, VT 05609

FOR BOEHRINGER INGELHEIM PHARMACEUTICALS, INC.

By: _____ Date: 12/13/17

J. Sedwick Sollers, III, Esq.
Mark Jensen, Esq.
Brandt A. Leibe. Esq.
Daniel C. Sale, Esq.
King & Spalding LLP

Counsel for Boehringer Ingelheim Pharmaceuticals, Inc.

By: _____ Date: 12/18/17

Kevin A. Lumpkin, Esq.
SHEEHEY FURLONG & BEHM P.C.
30 Main Street, 6th Floor
P.O. Box 66
Burlington, VT 05402-0066
(802) 864-9891
klumpkin@sheeheyvt.com

Counsel for Boehringer Ingelheim Pharmaceuticals, Inc.

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

STATE OF VERMONT, Plaintiff, v. BOEHRINGER INGELHEIM PHARMACEUTICALS, INC., Defendant.	CIVIL DIVISION Docket No. 929-12-17 Wncv

FINAL CONSENT JUDGMENT

Plaintiff the State of Vermont has filed a Complaint for a permanent injunction and other relief in this matter pursuant to 9 V.S.A. § 2451, *et seq.* of the Vermont Consumer Protection Act ("CPA"), and Plaintiff, by its counsel, and Defendant Boehringer Ingelheim Pharmaceuticals, Inc. (BIPI), by its counsel, have agreed to the entry of this Final Consent Judgment by the Court without trial or adjudication of any issue of fact or law, and without finding or admission of wrongdoing or liability of any kind of any violation of the CPA as alleged by Plaintiff.

IT IS HEREBY ORDERED THAT:

1. PARTIES

1.1 Plaintiff, the State of Vermont is charged with the enforcement of the CPA.

1.2 Defendant, Boehringer Ingelheim Pharmaceuticals, Inc., is a Delaware corporation with its principal place of business at 900 Ridgebury Road in Ridgefield,

Connecticut. At all relevant times, BIPI did business in Vermont by marketing, selling, and Promoting the drugs Aggrenox, Atrovent, Combivent, and Micardis (hereinafter the "Covered Products").

2. PREAMBLE

2.1 BIPI represents it voluntarily established a compliance program that is applicable to all BIPI employees prior to the execution of this Judgment.

2.2 BIPI further represents its compliance program includes a Compliance Officer; a Code of Conduct; written policies and procedures; education and training initiatives; a disclosure program that allows for confidential disclosure and investigation of potential compliance violations and appropriate disciplinary procedures; and regular internal auditing procedures.

3. FINDINGS

3.1 This Court has jurisdiction over the subject matter of this lawsuit and over all parties.

3.2 The terms of this Judgment shall be governed by the laws of the State of Vermont.

3.3 Entry of this Judgment is in the public interest and reflects a negotiated agreement among the parties.

3.4 The parties have agreed to resolve the issues resulting from the Covered Conduct by entering into this Judgment.

3.5 BIPI is willing to enter into this Judgment regarding the Covered Conduct in order to resolve the Signatory Attorney General's concerns under the State Consumer Protection Laws as to the matters addressed in this Judgment and thereby avoid significant expense, inconvenience, and uncertainty.

3.6 BIPI is entering into this Judgment solely for the purpose of settlement, and nothing contained herein may be taken as or construed to be an admission or concession of any

violation of law, or regulation, or of any other matter of fact or law, or of any liability or wrongdoing, including allegations in the Complaint, all of which BIPI expressly denies. BIPI does not admit any violation of law, and does not admit any wrongdoing that was or could have been alleged by the Signatory Attorney General before the date of the Judgment. No part of this Judgment, including its statements and commitments, shall constitute evidence of any liability, fault, or wrongdoing by BIPI.

3.7 This Judgment shall not be construed or used as a waiver or limitation of any defense otherwise available to BIPI in any action, or of BIPI's right to defend itself from, or make any arguments in, any private individual, regulatory, governmental, or class claims or suits relating to the subject matter or terms of this Judgment. Nothing in this Judgment shall waive, release, or otherwise affect any claims, defenses, or positions BIPI may have in connection with any investigations, claims, or other matters the State/Commonwealth is not releasing hereunder. This Judgment is made without trial or adjudication of any issue of fact or law or finding of liability of any kind. It is the intent of the parties that this Judgment shall not be binding or admissible in any other matter, including, but not limited to, any investigation or litigation, other than in connection with the enforcement of this Judgment. Unless otherwise provided under state law, no part of this Judgment shall create a private cause of action or confer any right to any third party for violation of any federal or state statute except that a State may file an action to enforce the terms of this Judgment. Notwithstanding the foregoing, the State of Vermont may file an action to enforce the terms of this Judgment.

3.8 This Judgment (or any portion thereof) shall in no way be construed to prohibit, limit, or restrict BIPI from making representations with respect to the Covered Products that are permitted or authorized under federal law, the Federal Food, Drug & Cosmetic Act ("FDCA"),

21 U.S.C. § 301 et seq., U.S. Food and Drug Administration ("FDA") regulations, or FDA Guidances for Industry, currently issued or as revised. Further, the Judgment shall in no way prohibit, limit, or restrict BIPI from making representations with respect to the Covered Products that are required or authorized by, or consistent with the FDA-approved Labeling or prescribing information, or by any Investigational New Drug Application, New Drug Application, Supplemental New Drug Application, or Abbreviated New Drug Application filed with the FDA so long as the representation, taken in its entirety, is not false, misleading or deceptive.

3.9 Nothing in this Judgment shall require BIPI to:

(a) take any action that is prohibited by the Food, Drug and Cosmetic Act, 21 U.S.C. § 301 *et seq.* ("FDCA") or any regulation promulgated thereunder, or by the FDA; or

(b) fail to take any action that is required by the FDCA or any regulation promulgated thereunder, or by the FDA.

4. DEFINITIONS

The following definitions shall be used in construing this Judgment:

4.1 "BIPI" means Boehringer Ingelheim Pharmaceuticals, Inc., including all of its past and present subsidiaries, predecessors, successors, and assigns.

4.2 "BIPI Marketing" shall mean BIPI personnel responsible for marketing Covered Products in the United States.

4.3 "BIPI Medical" shall mean BIPI personnel who are highly trained experts with specialized scientific or medical knowledge whose roles involve the provision of specialized medical or scientific information, scientific analysis, and/or scientific information to HCPs but excludes anyone performing sales, marketing, or other commercial roles.

4.4 "BIPI Sales" shall mean the BIPI sales force responsible for sales of Covered Products in the United States, including, but not limited to, the field force and all management personnel such as district managers, regional managers, vice president(s) over sales, and president over sales.

4.5 "Clear(ly) and Conspicuous(ly)" shall mean, with respect to a disclosure or information presented, that such information meets requirements of the FDCA, the requirements of FDA regulations, and the recommended actions in FDA Guidances for Industry, including FDA's "Guidance for Industry: Presenting Risk Information in Prescription Drug and Medical Device Promotion," or as revised.

4.6 "Covered Conduct" shall mean BIPI's Promotional and marketing practices, and dissemination of information and remuneration to HCPs regarding the Covered Products through the Effective Date of the Judgment.

4.7 "Covered Product" shall mean BIPI drugs: Aggrenox, Atrovent, Combivent, and Micardis, which have all been approved by FDA.

4.8 "Effective Date" shall mean the date on which a copy of this Judgment, duly executed by BIPI and by the Signatory Attorney General, is approved by, and becomes a Judgment of the Court.

4.9 "FDA Guidances for Industry" shall mean documents, as currently drafted or as revised, issued by the FDA pursuant to 21 U.S.C. §371(h) that represent the FDA's current thinking on a topic.

4.10 "HCP" shall mean any physician or other health care practitioner, who is licensed to provide health care services or to prescribe pharmaceutical products.

4.11 "Labeling" shall mean all labels and other written, printed, or graphic matter (a) upon any article or any of its containers or wrappers, or (b) accompanying such article.

4.12 "Medical Information Response(s)" shall mean a non-Promotional, scientific communication to address an Unsolicited Request for medical information from a HCP.

4.13 "Multistate Executive Committee" shall mean the Attorneys General and their staffs representing Arizona, the District of Columbia, Illinois, Indiana, Kansas, Nevada, Pennsylvania, Tennessee, and Texas.

4.14 "Multistate Working Group" shall mean the Attorneys General and their staffs representing Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, the District of Columbia, Florida, Georgia, Hawaii[1], 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[2], Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

4.15 "Off-Label" shall mean a use, including indication, dosage, population, and/or method of administration, not consistent with the use approved by the FDA in the Labeling for a Covered Product at the time information regarding such use was communicated, or at the time the conduct occurred.

---

[1] Hawaii is being 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, the entire group will be referred to as the "Attorneys General," and such designation, as it includes Hawaii, refers to the Executive Director of the State of Hawaii Office of Consumer Protection.

[2] The Utah Attorney General's Office represents the Utah Division of Consumer Protection (Division), the state agency charged with enforcement of the Consumer Sales Practices Act, in this action, but is not a party itself. As to Utah, the definition of "Attorneys General" means the Utah Attorney General as counsel to the Division.

4.16 "Promotional," "Promoting," or "Promote" shall mean representations made to HCPs, patients, consumers, payors, and other customers, about a Covered Product and other practices intended to increase sales in the United States or that attempt to influence prescribing practices of HCPs in the United States, including direct-to-consumer.

4.17 "Promotional Materials" shall mean any item used to Promote a Covered Product.

4.18 "Promotional Speaker(s)" shall mean a HCP speaker engaged by or on behalf of BIPI to Promote a Covered Product in the United States.

4.19 "Reprints Containing Off-Label Information" shall mean articles or reprints from a scientific or medical journal, as defined in 21 C.F.R. 99.3(j), or reference publication, as defined in 21 C.F.R. 99.3(i), describing an Off-Label use of a Covered Product.

4.20 "Signatory Attorney General" shall mean the Attorney General of Vermont, or his authorized designee, who has agreed to this Judgment.

4.21 "State Consumer Protection Laws" shall mean the CPA.

4.22 "Unsolicited Request" shall mean a request for information communicated to an agent of BIPI that has not been prompted by or on behalf of BIPI.

4.23 Any reference to a written document shall mean a physical paper copy of the document, an electronic version of the document, or electronic access to such document.

5. COMPLIANCE PROVISIONS

The following Compliance Provisions, Paragraphs 5.3 through 5.24, shall apply for five (5) years from the Effective Date of this Judgment.

Promotional Activities

5.1 BIPI shall not make, or cause to be made, any written or oral claim that is false, misleading, or deceptive regarding any Covered Product.

5.2 BIPI shall not represent that any Covered Product has any sponsorship, approval, characteristics, ingredients, uses, benefits, quantities, or qualities that it does not have.

5.3 BIPI shall not promote any Covered Product for any Off-Label use.

5.4 In Promotional Materials for Covered Products, BIPI shall Clearly and Conspicuously disclose the risks associated with the Covered Products as set forth in the products' Labeling and shall present information about effectiveness and risk in a balanced manner.

5.5 BIPI shall require that all Promotional Speakers for any Covered Product comply with BIPI's obligations contained in this Judgment.

5.6 BIPI shall notify BIPI Sales promptly of any warning letter received from the FDA that affects the conduct of any sales representative in Promoting the relevant Covered Product and shall promptly disseminate a description of the concerns described in the warning letter.

5.7 BIPI shall not Promote a Covered Product by misrepresenting any clinical treatment guideline in a manner that suggests a Covered Product is approved for uses not consistent with the FDA-approved prescribing information.

Product Sampling

5.8 BIPI shall provide samples of a Covered Product only to those HCPs whose clinical practice is consistent with the product's FDA-approved Labeling.

5.9 If a HCP whose clinical practice is inconsistent with a Covered Product's Labeling requests samples of that Covered Product, BIPI personnel shall refer the HCP to BIPI Medical where the HCP can speak directly with a BIPI Medical representative who will provide answers to the HCP's questions about the Covered Product, and BIPI may provide him/her with samples only if appropriate (i.e., if the HCP requests the samples for an FDA-approved [on-label] use).

Financial Incentives to BIPI Sales and/or BIPI Marketing

5.10 BIPI's financial incentives shall be designed to ensure that BIPI Sales and/or BIPI Marketing are not motivated to engage in improper Promotion, sales, and marketing of Covered Products.

5.11 BIPI's financial incentives shall not include mechanisms to provide incentive compensation for sales that may indicate Off-Label use of any Covered Product.

Dissemination and Exchange of Medical Information

5.12 The content of BIPI's communications concerning Off-Label uses of a Covered Product shall not be false, misleading, or deceptive. BIPI shall not knowingly disseminate any Medical Information Response, including one that describes any Off-Label use of a Covered Product, unless such information and materials comply with the standards in applicable FDA regulations and with recommendations in FDA Guidances for Industry.

5.13 BIPI Sales and BIPI Marketing shall not develop Medical Information Responses regarding a Covered Product.

5.14 Medical Information Responses to Unsolicited Requests for Off-Label information regarding a Covered Product may be disseminated only by BIPI Medical, except in circumstances implicating public health or safety issues.

5.15 BIPI Medical shall have ultimate responsibility for developing and approving all Medical Information Responses regarding a Covered Product. Additional approvals may be provided by BIPI's legal department. BIPI shall not distribute any such materials unless:

(a) clinically relevant information is included in these materials to provide scientific balance;

(b) data in these materials are presented in an unbiased, non-Promotional manner; and

(c) these materials are Clearly and Conspicuously distinguishable from sales aids and other Promotional Materials.

5.16 Nothing in this subsection shall prohibit BIPI Medical from disseminating materials that are permitted to be distributed under Federal law, Federal regulations, or FDA published Guidance, unless false, misleading, or deceptive.

Responses to Unsolicited Requests for Off-Label Information

5.17 If BIPI elects to respond to an Unsolicited Request for Off-Label information regarding a Covered Product, BIPI Medical shall provide specific, accurate, objective, and scientifically balanced responses. Any such response shall not Promote a Covered Product for any Off-Label use.

5.18 Any written BIPI response to an Unsolicited Request for Off-Label information regarding a Covered Product shall be a Medical Information Response and shall include:

(a) a copy of the FDA-required Labeling, if any, for the Covered Product (e.g., FDA-approved package insert and, if the response is for a consumer, FDA-approved patient Labeling);

(b) a prominent statement notifying the recipient that the FDA has not approved or cleared the Covered Product as safe and effective for the Off-Label use addressed in the accompanying materials;

(c) a prominent statement disclosing the uses for which FDA has approved or cleared the Covered Product; and

(d) a report containing the results of a reasonable literature search using terms from the request.

5.19 BIPI Sales and BIPI Marketing may respond orally to an Unsolicited Request for Off-Label information regarding a Covered Product only by offering to refer the request to BIPI Medical or by offering to put the HCP in touch with BIPI Medical.

Reprints Containing Off-Label Information

5.20 BIPI shall not disseminate information describing any Off-Label or unapproved use of a Covered Product, unless such information and materials comply with the standards in applicable FDA regulations and with recommendations in FDA Guidances for Industry, including FDA's "Guidance for Industry: Responding to Unsolicited Requests for Off-Label Information About Prescription Drugs and Medical Devices" and FDA's "Guidance for Industry: Distributing Scientific and Medical Publications on Unapproved New Uses – Recommended Practices," or as revised.

5.21 BIPI Medical shall be responsible for the identification, selection, approval and dissemination of Reprints Containing Off-Label Information regarding a Covered Product.

5.22 Reprints Containing Off-Label Information regarding a Covered Product:

(a) shall be accompanied by the FDA approved Labeling for the Covered Product or a prominently displayed and Clearly and Conspicuously described hyperlink that

will provide the reader with such information;

(b) shall contain a Clear and Conspicuous disclosure in a prominent location, which would include the first page or as a cover page where practicable, indicating that the article discusses Off-Label information; and

(c) shall not be referred to or used in a Promotional manner.

5.23 Reprints Containing Off-Label Information regarding a Covered Product may only be disseminated if approved by BIPI Medical to HCPs.

5.24 This section of the Judgment does not apply to reprints containing only incidental references to Off-Label information. If reprints have an incidental reference to Off-Label information, such reprints shall contain the disclosures required by Paragraph 5.22 (a) and Paragraph 5.22 (b) in a prominent location, as defined above, and such incidental reference to Off-Label information shall not be referred to or used in a Promotional manner as prohibited by Paragraph 5.22 (c).

6. PAYMENT

6.1 No later than 30 days after the Effective Date of this Judgment, BIPI shall pay a total amount of Thirteen Million Five Hundred Thousand Dollars ($13,500,000) to be divided and paid by BIPI directly to each Signatory Attorney General of the Multistate Working Group in an amount to be designated by and in the sole discretion of the Multistate Executive Committee. Of that amount, Vermont shall receive one hundred thirty thousand, eight hundred sixty dollars and forty-one cents ($130, 860.41). Said payment shall be used by the States as attorneys' fees and other costs of investigation and litigation, or to be placed in, or applied to, the consumer protection enforcement fund, including future consumer protection enforcement, consumer education, litigation or local consumer aid fund or revolving fund, used to defray the costs of the inquiry leading hereto, or any lawful purpose, at the sole discretion of each Signatory

Attorney General, and in Vermont, pursuant to the Constitution of the State of Vermont, Ch. II § 27 and 32 V.S.A. § 462. The parties acknowledge that the payment described herein is not a fine, penalty, or payment in lieu thereof.

7. RELEASE

7.1 By its execution of this Judgment, the State of Vermont releases BIPI and all of its past and present subsidiaries, predecessors, successors, assigns, parents, affiliates, each of their current and former officers, directors, shareholders, employees, agents, contractors, and attorneys (collectively, the Released Parties) from the following: all civil claims, *parens patriae* claims, causes of action, damages, restitution, fines, attorney's fees, costs, and penalties that the Vermont Attorney General has asserted or could have asserted against the Released Parties under the above-cited consumer protection statutes or any common law claims concerning unfair, fraudulent, or deceptive trade practices other than those described in Paragraph 7.2 resulting from the Covered Conduct up to and including the Effective Date.

7.2 Notwithstanding any term of this Judgment, specifically reserved and excluded from the release in Paragraph 7.1 as to any entity or person, including Released Parties, are any and all of the following:

(a) any criminal liability that any person and/or entity, including Released Parties, has or may have to the State of Vermont;

(b) any civil or administrative liability that any person and/or entity, including Released Parties, has or may have to the State of Vermont not expressly covered by the release in Paragraph 7.1 above, including, but not limited to, any and all of the following claims:

(i) state or federal antitrust violations;

(ii) claims involving "best price," "average wholesale price," "wholesale acquisition cost," or any price-reporting practices;

(iii) Medicaid claims, including, but not limited to, federal Medicaid drug rebate statute violations, Medicaid fraud or abuse, and/or kickback violations related to any State's Medicaid program;

(iv) state false claims violations; and

(v) actions of state program payors of the State of Vermont arising from the purchase of a Covered Product, except for the release of civil penalties under 9 V.S.A. § 2451, et seq. of the CPA.

(c) any claims individual consumers have or may have under the CPA, and any common law claims individual consumers may have concerning unfair, fraudulent or deceptive trade practices, against any person and/or entity, including Released Parties.

8. DISPUTE RESOLUTION

8.1 For the purposes of resolving disputes with respect to compliance with this Judgment, should any of the Signatory Attorneys General have a reasonable basis to believe that BIPI has engaged in a practice that violates a provision of this Judgment subsequent to the Effective Date of this Judgment, then such Attorney General shall notify BIPI in writing of the specific objection, identify with particularity the provision of this Judgment that the practice appears to violate, and give BIPI 30 days to respond to the notification; provided, however, that a Signatory Attorney General may take any action if the Signatory Attorney General concludes that, because of the specific practice, a threat to the health or safety of the public requires immediate action. Upon receipt of written notice, BIPI shall provide a good-faith written response to the Attorney General notification, containing either a statement explaining why BIPI

believes it is in compliance with the Judgment, or a detailed explanation of how the alleged violation occurred and a statement explaining how BIPI intends to remedy the alleged breach. Nothing in this section shall be interpreted to limit the state's Civil Investigative Demand ("CID") or investigative subpoena authority, to the extent such authority exists under applicable law, and BIPI reserves all of its rights in responding to a CID or investigative subpoena issued pursuant to such authority.

8.2 Upon giving BIPI 30 days to respond to the notification described above, the Signatory Attorney General shall also be permitted reasonable access to inspect and copy relevant, non-privileged, non-work product records and documents in the possession, custody, or control of BIPI that relate to BIPI's compliance with each provision of this Judgment pursuant to that State's CID or investigative subpoena authority. If the Signatory Attorney General makes or requests copies of any documents during the course of that inspection, the Signatory Attorney General will provide a list of those documents to BIPI.

8.3 The Signatory Attorney General may assert any claim that BIPI has violated this Judgment in a separate civil action to enforce compliance with this Judgment, or may seek any other relief afforded by law, but only after providing BIPI an opportunity to respond to the notification described in Paragraph 8.1 above; provided, however, that the Signatory Attorney General may take any action if the Signatory Attorney General concludes that, because of the specific practice, a threat to the health or safety of the public requires immediate action.

9. GENERAL PROVISIONS

9.1 BIPI shall not cause third parties, acting on its behalf, to engage in practices from which BIPI is prohibited by this Judgment.

9.2 This Judgment does not constitute an approval by any of the Signatory Attorneys General of BIPI's business practices, and BIPI shall make no representation or claim to the

contrary.

9.3 Any failure by any party to this Judgment to insist upon the strict performance by any other party of any of the provisions of this Judgment shall not be deemed a waiver of any of the provisions of this Judgment, and such party, notwithstanding such failure, shall have the right thereafter to insist upon the specific performance of any and all of the provisions of this Judgment. This Judgment represents the full and complete terms of the settlement entered into by the parties hereto. In any action undertaken by the parties, no prior versions of this Judgment or any of its terms that were not entered by the Court in this Judgment, may be introduced for any purpose whatsoever.

9.4 This Court retains jurisdiction of this Judgment and the parties hereto for the purpose of enforcing and modifying this Judgment and for the purpose of granting such additional relief as may be necessary and appropriate.

9.5 This Judgment may be executed in counterparts, and a facsimile or .pdf signature shall be deemed to be, and shall have the same force and effect as, an original signature.

9.6 To the extent that any provision of this Judgment obligates BIPI to change any policy(ies) or procedure(s) and to the extent not already accomplished, BIPI shall implement the policy(ies) or procedure(s) as soon as reasonably practicable, but no later than 90 days after the Effective Date of this Judgment.

9.7 The parties agree that neither of them shall be deemed the drafter of this Judgment and that, in construing this Judgment, no provision hereof shall be construed in favor of one party on the ground that such provision was drafted by the other.

9.8 All notices under this Judgment shall be provided to the following via email and Overnight Mail:

For the State of Vermont:
Jill S. Abrams
Vermont Attorney General's Office
109 State Street
Montpelier, VT 05609

For Boehringer Ingelheim Pharmaceuticals, Inc.:

Wick Sollers
King & Spalding LLP
1700 Pennsylvania Avenue, N.W.
Washington, DC 20006
wsollers@kslaw.com

IT IS SO ORDERED, ADJUDGED AND DECREED.

_____
Date

_____
Presiding Judge

JOINTLY APPROVED AND
SUBMITTED FOR ENTRY

FOR PLAINTIFF, STATE OF VERMONT
THOMAS J. DONOVAN, JR.

_____ Date: Dec. 20, 2017
Jill S. Abrams
Vermont Attorney General's Office
109 State Street
Montpelier, VT 05609

FOR BOEHRINGER INGELHEIM PHARMACEUTICALS, INC.

By: _____ Date: 12/13/17

J. Sedwick Sollers, III, Esq.
Mark Jensen, Esq.
Brandt **A. Leibe. Esq.**
Daniel C. Sale, Esq.
King & Spalding LLP

*Counsel for Boehringer Ingelheim Pharmaceuticals, **Inc.***

By: _____ Date: 12/18/17

Kevin A. Lumpkin, Esq.
SHEEHEY FURLONG & BEHM P.C.
30 Main Street, 6th Floor
P.O. Box 66
Burlington, VT 05402-0066
(802) 864-9891
klumpkin@sheeheyvt.com

Counsel for Boehringer Ingelheim Pharmaceuticals, Inc.

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

In Re: CHARLES DESAUTELS) CIVIL DIVISION
) Docket No. 251-4-17 Wncv.

ASSURANCE OF DISCONTINUANCE

The State of Vermont, by and through Vermont Attorney General Thomas J. Donovan, Jr., and Charles Desautels ("Respondent"), hereby enter into this Assurance of Discontinuance ("AOD") pursuant to 9 V.S.A. § 2459.

Regulatory Framework

1. Lead-based paint in housing, the focus of the Vermont lead law, is a leading cause of childhood lead poisoning, which can result in adverse health effects, including decreases in IQ.
2. All paint in pre-1978 housing is presumed to be lead-based unless a certified inspector has determined that it is not lead-based. 18 V.S.A. § 1759(a).
3. All paint in rental target housing is "presumed to be lead-based unless a lead inspector or lead risk assessor has determined that it is not lead-based." 18 V.S.A. § 1760(a).
4. The lead law requires that essential maintenance practices ("EMPs") specified in 18 V.S.A. § 1759 be performed at all pre-1978 rental housing.
5. EMPs include, but are not limited to, installing window well inserts, visually inspecting properties at least annually for deteriorated paint, restoring surfaces to be free of deteriorated paint within 30 days after such paint has been visually identified

Office of the ATTORNEY GENERAL
109 State Street
Montpelier, VT 05609

or reported to the owner, and posting lead-based paint hazard information in a prominent place. 18 V.S.A. § 1759(a) (2), (4) and (7).

6. The EMP requirements also mandate that an owner of rental target housing file affidavits or compliance statements attesting to EMP performance with the Vermont Department of Health and with the owner's insurance carrier. 18 V.S.A. § 1759(b).
7. A violation of the lead law requirements may result in a maximum civil penalty of $10,000.00. 18 V.S.A. § 130(b)(6). Each day that a violation continues is a separate violation. 18 V.S.A. § 130(b)(6).
8. The Vermont Consumer Protection Act, 9 V.S.A Chapter 63, prohibits unfair and deceptive acts and practices, which includes the offering for rent, or the renting of, target housing that is noncompliant with the lead law.
9. Violations of the Consumer Protection Act are subject to a civil penalty of up to $10,000.00 per violation. 9 V.S.A. § 2458(b)(1). Each day that a violation continues is a separate violation.

Respondent's Rental Housing and Lead Compliance Practices

10. Respondent is the owner of thirteen rental properties located in Richford and Enosburg Falls, Vermont (see Attachment A, collectively hereafter "the Properties").
11. The Properties were all constructed prior to 1978, and therefore, are pre-1978 "rental target housing" within the meaning of the Vermont lead law, 18 V.S.A. § 1751(23), and are all subject to the requirements of 18 V.S.A. Chapter 38.
12. Respondent has in the past and continues presently to rent and offer for rent units in the Properties.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

13. On May 19, 2015 the Vermont Department of Health sent a "Notice of Non-Compliance" indicating that Respondent had not filed an "EMP Rental Property Compliance Statement" for the Properties. The Department allowed for 30 days for Respondent to file the necessary statements.

14. Respondent did not file the EMP compliance statements within 30 days.

15. As of January 2017, Respondent has not filed current EMP compliance statements for all of the Properties.

16. Respondent admits the truth of the facts described in ¶¶ 10-15.

The State's Allegations

17. The Vermont Attorney General's Office alleges the following violations of the Consumer Protection Act and Lead Law:

    a. Failing to file EMP compliance statements for rental properties.

18. The State of Vermont alleges that the above behavior constitutes unfair and deceptive acts and practices under 9 V.S.A. § 2453.

Assurances and Relief

In lieu of instituting an action or proceeding against Respondent, the Attorney General and Respondent are willing to accept this AOD pursuant to 9 V.S.A. § 2459. Accordingly, the parties agree as follows:

19. Respondent shall fully and timely comply with the requirements of the Vermont lead law, 18 V.S.A., Chapter 38, as long as they maintain any ownership or property management interest in the Properties and in any other pre-1978 rental housing in which they currently have, or later acquire, an ownership or property management interest.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

20. By May 15, 2017, Respondent shall complete all EMP inspections and work of the Properties (as specified in 18 V.S.A. § 1759), giving priority to the Properties where a child age 6 or under is residing. Pursuant to 18 V.S.A. § 1759(a)(3), exterior work of the properties may be postponed until May 31, 2017, so long as access to exterior surfaces and components of the Properties with lead hazards and areas directly below the deteriorated surfaces are clearly restricted. All interior work must be completed by the May 15, 2017 deadline. If Respondent requires additional time to complete the work, Respondent will contact the Attorney General's Office before the expiration of the above deadlines and provide a detailed justification for any extension.

21. Within one week of completion of the EMP work at the Properties described in the paragraph above, Respondent will file with the Vermont Department of Health, Respondent's insurance carrier and with the Office of the Attorney General, a completed EMP compliance statement for all Properties, and will give a copy of the compliance statement to an adult in each rented unit of all Properties. The copy for the Office of the Attorney General shall be sent to: *Justin Kolber, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.*

22. In the event Respondent wishes to rent a unit which becomes vacant in any of Respondent's pre-1978 rental housing before such housing is made EMP compliant, Respondent shall provide advance written notice of the intent to rent to the Office of the Attorney General at the address listed above. Respondent's advance written notice shall also: (1) verify that the interior of the specific unit to be rented is EMP

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

compliant; (2) provide an update as to any remaining EMP work to be performed at the property, including the date by which the entire property will be EMP compliant. Otherwise, Respondent shall not rent, or offer for rent, any unit which becomes vacant in any of property owned or managed by Respondent that is not EMP compliant until such time as the EMP work is complete and the EMP compliance statement is distributed as described above.

23. Respondent shall pay the sum of $15,000 in civil penalties and costs for the failure to file EMP compliance statements, as follows:

    a. Respondent shall pay three thousand dollars by May 31, 2017 and two thousand dollars by September 30, 2017. All payments shall be a single check payable to the "State of Vermont" and sent to the Office of the Attorney General at the address listed in paragraph 21; and

    b. Respondent shall expend at least ten thousand dollars ($10,000), including the actual cost of materials and the actual cost of labor, on lead hazard reduction improvements at any or all of the Properties described herein.

24. Respondent shall pay the costs of any follow-up compliance inspections as determined by the Attorney General's Office.

Other Terms

25. This AOD is binding on Respondent, however, sale of any pre-1978 rental property may not occur unless Respondent has complied with all obligations under this AOD, or this AOD is amended in writing to transfer to the buyer or other transferee all remaining obligations.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

26. Transfer of ownership of any of Respondent's pre-1978 rental properties shall be consistent with Vermont law, including the provisions of 18 V.S.A. § 1767 specifically relating to the transfer of ownership of pre-1978 rental housing.
27. This AOD shall not affect marketability of title.
28. Nothing in this AOD in any way affects Respondent's other obligations under state, local, or federal law.
29. In addition to any other penalties or relief which might be appropriate under Vermont law, any future failure by Respondent to comply with the terms of this AOD shall be subject to a liquidated civil penalty paid to the State of Vermont in the amount of at least $5,000 and not more than $10,000.

SIGNATURES APPEAR ON NEXT PAGE

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

DATED at Montpelier, Vermont this 17th day of April, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____
Justin Kolber
Assistant Attorney General
Office of the Attorney General
109 State Street
Montpelier, VT 05609
(802) 828-5620
justin.kolber@vermont.gov

DATED at Richford, Vermont this 18 day of April, 2017.

CHARLES DESAUTELS

By: _____
Charles Desautels

Claude J Desautels
PO Box 334
Richford VT 05476

Office of the
ATTORNEY
GENERAL
109 State Street
Montpelier, VT
05609

Attachment A – List of Respondent's Rental Properties in Richford and Enosburg Falls, VT

1. 512 East Richford Slide Road
2. 14 Elm Avenue
3. 278 Golf Course Road
4. 215 Main Street
5. 145 Province Street
6. 5 River Street
7. 11 River Street
8. 50 River Street
9. 60 River Street
10. 13 Troy Street
11. 49 Troy Street
12. 487 Main Street, Enosburg Falls
13. 123 Elm Street, Enosburg Falls

Total: 13 properties

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

In Re: CHRISTOPHER WILK	)	CIVIL DIVISION
	)	Docket No. _____

ASSURANCE OF DISCONTINUANCE

The State of Vermont, by and through Vermont Attorney General Thomas J. Donovan, Jr., and Christopher Wilk ("Respondent"), hereby enter into this Assurance of Discontinuance ("AOD") pursuant to 9 V.S.A. § 2459.

Regulatory Framework

1. Lead-based paint in housing, the focus of the Vermont lead law, is a leading cause of childhood lead poisoning, which can result in adverse health effects, including decreases in IQ.
2. All paint in pre-1978 housing is presumed to be lead-based unless a certified inspector has determined that it is not lead-based. 18 V.S.A. § 1759(a).
3. All paint in rental target housing is "presumed to be lead-based unless a lead inspector or lead risk assessor has determined that it is not lead-based." 18 V.S.A. § 1760(a).
4. The lead law requires that essential maintenance practices ("EMPs") specified in 18 V.S.A. § 1759 be performed at all pre-1978 rental housing.
5. EMPs include, but are not limited to, installing window well inserts, visually inspecting properties at least annually for deteriorated paint, restoring surfaces to be free of deteriorated paint within 30 days after such paint has been visually identified

Office of the ATTORNEY GENERAL
109 State Street
Montpelier, VT 05609

or reported to the owner, and posting lead-based paint hazard information in a prominent place. 18 V.S.A. § 1759(a) (2), (4) and (7).

6. The EMP requirements also mandate that an owner of rental target housing file affidavits or compliance statements attesting to EMP performance with the Vermont Department of Health and with the owner's insurance carrier. 18 V.S.A. § 1759(b).
7. A violation of the lead law requirements may result in a maximum civil penalty of $10,000.00. 18 V.S.A. § 130(b)(6). Each day that a violation continues is a separate violation. 18 V.S.A. § 130(b)(6).
8. The Vermont Consumer Protection Act, 9 V.S.A Chapter 63, prohibits unfair and deceptive acts and practices, which includes the offering for rent, or the renting of, target housing that is noncompliant with the lead law.
9. Violations of the Consumer Protection Act are subject to a civil penalty of up to $10,000.00 per violation. 9 V.S.A. § 2458(b)(1). Each day that a violation continues is a separate violation.

Respondent's Rental Housing and Lead Compliance Practices

10. Respondent is the owner of at least one rental property, containing 7 rental units, located at 51 West Street located in Rutland, Vermont ("the Property").
11. The Property was constructed prior to 1978, and therefore, is pre-1978 "rental target housing" within the meaning of the Vermont lead law, 18 V.S.A. § 1751(23), and is all subject to the requirements of 18 V.S.A. Chapter 38.
12. Respondent has in the past and continues presently to rent and offer for rent units in the Property.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

13. On January 9, 2017, Respondent filed with the Vermont Department of Health an "EMP Rental Property Compliance Statement" for 51 West Street.

14. The EMP Statement represented that Respondent performed EMPs at 51 West Street on September 12, 2016.

15. The EMP Statement specifically certified that Respondent:

    a. visually inspected exterior surfaces and outbuildings;

    b. stabilized exterior paint; and

    c. did not identify deteriorated paint exceeding 1 square foot on exterior surfaces of the buildings.

16. The EMP Statement was signed by Christopher Wilk and certified that "all information provided on this form is true and accurate" and acknowledged that "providing false, incomplete or inaccurate information on this form is unlawful and is punishable by civil and criminal penalties pursuant to Vermont law."

17. On January 17, 2017, Vermont Department of Health staff inspected the exterior of 51 West Street and documented (via photographs) deteriorated paint exceeding more than 1 square foot on the property's exterior surface.

18. Respondent admits the truth of the facts described in ¶¶ 10-17.

The State's Allegations

19. The Vermont Attorney General's Office alleges the following violations of the Consumer Protection Act and Lead Law:

    a. Submitting a false EMP compliance statement and inaccurately representing that the property was in compliance with the lead law.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

20. The State of Vermont alleges that the above behavior constitutes unfair and deceptive acts and practices under 9 V.S.A. § 2453.

Assurances and Relief

In lieu of instituting an action or proceeding against Respondent, the Attorney General and Respondent are willing to accept this AOD pursuant to 9 V.S.A. § 2459. Accordingly, the parties agree as follows:

21. Respondent shall fully and timely comply with the requirements of the Vermont lead law, 18 V.S.A., Chapter 38, as long as they maintain any ownership or property management interest in the Properties and in any other pre-1978 rental housing in which they currently have, or later acquire, an ownership or property management interest.

22. By June 20, 2017, Respondent shall provide to the Attorney General's Office a detailed plan for completing all EMP inspections and work of the Properties (as specified in 18 V.S.A. § 1759), including the names of EMP-certified contractors that she has contacted or will contact and estimated timeframes to complete the EMP work. By June 30, 2017, all exterior EMP work of the Properties shall be completed in a lead-safe manner in accordance with 18 V.S.A. § 1760. If Respondent requires additional time to complete the work, Respondent will contact the Department of Health to request an extension of time agreement before the expiration of the above deadlines and provide a detailed justification for any extension. Any extension will be granted only for the exterior of the Properties; all interior work must be completed promptly.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

23. Within one week of completion of the EMP work at the Properties described in the paragraph above, Respondent will file with the Vermont Department of Health, Respondent's insurance carrier and with the Office of the Attorney General, a completed EMP compliance statement for all Properties, and will give a copy of the compliance statement to an adult in each rented unit of all Properties. The copy for the Office of the Attorney General shall be sent to: Justin Kolber, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.

24. In the event Respondent wishes to rent a unit which becomes vacant in any of Respondent's pre-1978 rental housing before such housing is made EMP compliant, Respondent shall provide advance written notice of the intent to rent to the Office of the Attorney General at the address listed above. Respondent's advance written notice shall also: (1) verify that the interior of the specific unit to be rented is EMP compliant; (2) provide an update as to any remaining EMP work to be performed at the property, including the date by which the entire property will be EMP compliant. Otherwise, Respondent shall not rent, or offer for rent, any unit which becomes vacant in any of property owned or managed by Respondent that is not EMP compliant until such time as the EMP work is complete and the EMP compliance statement is distributed as described above.

25. Respondent shall pay the sum of $5,000 in civil penalties and costs for the filing of a false EMP compliance statement. Based on Respondent's demonstrated inability to pay the full penalty and upon review of financial information provided to the State by Respondent, the State agrees to accept a reduced penalty of $500. Payment of the

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

$500 shall be made to the "State of Vermont" and sent to the following address: Justin E. Kolber, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609. Respondent shall also expend at least three thousand dollars ($3,000), including the actual cost of materials and the actual cost of labor, on lead hazard reduction improvements at the Property described herein.

Other Terms

26. This AOD is binding on Respondent, however, sale of any pre-1978 rental property may not occur unless Respondent has complied with all obligations under this AOD, or this AOD is amended in writing to transfer to the buyer or other transferee all remaining obligations.
27. Transfer of ownership of any of Respondent's pre-1978 rental properties shall be consistent with Vermont law, including the provisions of 18 V.S.A. § 1767 specifically relating to the transfer of ownership of pre-1978 rental housing.
28. This AOD shall not affect marketability of title.
29. Nothing in this AOD in any way affects Respondent's other obligations under state, local, or federal law.
30. In addition to any other penalties or relief which might be appropriate under Vermont law, any future failure by Respondent to comply with the terms of this AOD shall be subject to a liquidated civil penalty paid to the State of Vermont in the amount of at least $5,000 and not more than $10,000.

SIGNATURES APPEAR ON NEXT PAGE

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

DATED at Montpelier, Vermont this 12th day of June, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____
Justin E. Kolber
Assistant Attorney General
Office of the Attorney General
109 State Street
Montpelier, VT 05609
(802) 828-5620
justin.kolber@vermont.gov

DATED at Center Rutland, Vermont this 9 day of June, 2017.

CHRISTOPHER WILK

By: _____
Christopher Wilk

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

In Re: DAVID BUSHEY) CIVIL DIVISION
) Docket No. 432-7-17 Wncv

ASSURANCE OF DISCONTINUANCE

The State of Vermont, by and through Vermont Attorney General Thomas J. Donovan, Jr., and David Bushey ("Respondent"), hereby enter into this Assurance of Discontinuance ("AOD") pursuant to 9 V.S.A. § 2459.

Regulatory Framework

1. Lead-based paint in housing, the focus of the Vermont lead law, is a leading cause of childhood lead poisoning, which can result in adverse health effects, including decreases in IQ.
2. All paint in pre-1978 housing is presumed to be lead-based unless a certified inspector has determined that it is not lead-based. 18 V.S.A. § 1759(a).
3. All paint in rental target housing is "presumed to be lead-based unless a lead inspector or lead risk assessor has determined that it is not lead-based." 18 V.S.A. § 1760(a).
4. The lead law requires that essential maintenance practices ("EMPs") specified in 18 V.S.A. § 1759 be performed at all pre-1978 rental housing.
5. EMPs include, but are not limited to, installing window well inserts, visually inspecting properties at least annually for deteriorated paint, restoring surfaces to be free of deteriorated paint within 30 days after such paint has been visually identified

Office of the ATTORNEY GENERAL
109 State Street
Montpelier, VT 05609

or reported to the owner, and posting lead-based paint hazard information in a prominent place. 18 V.S.A. § 1759(a) (2), (4) and (7).

6. The EMP requirements also mandate that an owner of rental target housing file affidavits or compliance statements attesting to EMP performance with the Vermont Department of Health and with the owner's insurance carrier. 18 V.S.A. § 1759(b).
7. A violation of the lead law requirements may result in a maximum civil penalty of $10,000.00. 18 V.S.A. § 130(b)(6). Each day that a violation continues is a separate violation. 18 V.S.A. § 130(b)(6).
8. The Vermont Consumer Protection Act, 9 V.S.A Chapter 63, prohibits unfair and deceptive acts and practices, which includes the offering for rent, or the renting of, target housing that is noncompliant with the lead law.
9. Violations of the Consumer Protection Act are subject to a civil penalty of up to $10,000.00 per violation. 9 V.S.A. § 2458(b)(1). Each day that a violation continues is a separate violation.

Respondent's Rental Housing and Lead Compliance Practices

10. Respondent is the owner of seven rental properties located at: 42 Cedar Street; 44 Cedar Street; 46 Cedar Street; 24 Huntington Street; 26 Huntington Street; and 17 Walnut Street, all located in St. Albans (collectively, "the Properties").
11. The Properties were all constructed prior to 1978, and therefore, are pre-1978 "rental target housing" within the meaning of the Vermont lead law, 18 V.S.A. § 1751(23), and are all subject to the requirements of 18 V.S.A. Chapter 38.
12. Respondent has in the past and continues presently to rent and offer for rent units in the Properties.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

13. On November 29, 2016, the Vermont Department of Health sent a "Notice of Non-Compliance" indicating that Respondent had not filed an "EMP Rental Property Compliance Statement" for the properties at 42-46 Cedar Street. The Department allowed for 30 days for Respondent to file the necessary statements.

14. Respondent did not respond to the 30-day Notice, and did not file EMP compliance statements within 30 days.

15. As of June 2017, Respondent has not filed current EMP compliance statements for all six rental properties.

16. Respondent admits the truth of the facts described in ¶¶ 10-15.

The State's Allegations

17. The Vermont Attorney General's Office alleges the following violations of the Consumer Protection Act and Lead Law:

    a. Failing to file EMP compliance statements for rental properties.

18. The State of Vermont alleges that the above behavior constitutes unfair and deceptive acts and practices under 9 V.S.A. § 2453.

Assurances and Relief

In lieu of instituting an action or proceeding against Respondent, the Attorney General and Respondent are willing to accept this AOD pursuant to 9 V.S.A. § 2459. Accordingly, the parties agree as follows:

19. Respondent shall fully and timely comply with the requirements of the Vermont lead law, 18 V.S.A., Chapter 38, as long as they maintain any ownership or property management interest in the Properties and in any other pre-1978 rental housing in

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

which they currently have, or later acquire, an ownership or property management interest.

20. By July 31, 2017, Respondent shall complete all EMP inspections and work of the Properties (as specified in 18 V.S.A. § 1759), giving priority to the Properties where a child age 6 or under is residing. If Respondent requires additional time to complete the work, Respondent will contact the Attorney General's Office before the expiration of the above deadlines and provide a detailed justification for any extension.

21. Within one week of completion of the EMP work at the Properties described in the paragraph above, Respondent will file with the Vermont Department of Health, Respondent's insurance carrier and with the Office of the Attorney General, a completed EMP compliance statement for all Properties, and will give a copy of the compliance statement to an adult in each rented unit of all Properties. The copy for the Office of the Attorney General shall be sent to: *Justin Kolber, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.*

22. In the event Respondent wishes to rent a unit which becomes vacant in any of Respondent's pre-1978 rental housing before such housing is made EMP compliant, Respondent shall provide advance written notice of the intent to rent to the Office of the Attorney General at the address listed above. Respondent's advance written notice shall also: (1) verify that the interior of the specific unit to be rented is EMP compliant; (2) provide an update as to any remaining EMP work to be performed at the property, including the date by which the entire property will be EMP compliant.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

Otherwise, Respondent shall not rent, or offer for rent, any unit which becomes vacant in any of property owned or managed by Respondent that is not EMP compliant until such time as the EMP work is complete and the EMP compliance statement is distributed as described above.

23. Respondent shall pay the sum of $5,000 in civil penalties and costs for the failure to file EMP compliance statements. Based on Respondent's demonstrated inability to pay the full penalty and upon review of financial information provided to the State by Respondent, the State agrees to accept a reduced penalty of $1,000. Payment of the $1,000 shall be made to "the State of Vermont" and sent to the following address: *Justin E. Kolber, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609*. Respondent shall also expend at least three thousand dollars ($3,000), including the actual cost of materials and the actual cost of labor, on lead hazard reduction improvements at the Properties described herein.

24. Respondent shall pay the costs of any follow-up compliance inspections as determined by the Attorney General's Office.

Other Terms

25. This AOD is binding on Respondent, however, sale of any pre-1978 rental property may not occur unless Respondent has complied with all obligations under this AOD, or this AOD is amended in writing to transfer to the buyer or other transferee all remaining obligations.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

26. Transfer of ownership of any of Respondent's pre-1978 rental properties shall be consistent with Vermont law, including the provisions of 18 V.S.A. § 1767 specifically relating to the transfer of ownership of pre-1978 rental housing.
27. This AOD shall not affect marketability of title.
28. Nothing in this AOD in any way affects Respondent's other obligations under state, local, or federal law.
29. In addition to any other penalties or relief which might be appropriate under Vermont law, any future failure by Respondent to comply with the terms of this AOD shall be subject to a liquidated civil penalty paid to the State of Vermont in the amount of at least $5,000 and not more than $10,000.

SIGNATURES APPEAR ON NEXT PAGE

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

DATED at Montpelier, Vermont this 28th day of July, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____

Justin E. Kolber
Assistant Attorney General
Office of the Attorney General
109 State Street
Montpelier, VT 05609
(802) 828-5620
justin.kolber@vermont.gov

DATED at St. Albans, Vermont this 19th day of July, 2017.

DAVID BUSHEY

By: _____
David Bushey

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

JOSHUA R. DIAMOND
DEPUTY ATTORNEY GENERAL

WILLIAM E. GRIFFIN
CHIEF ASST. ATTORNEY GENERAL

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

TEL: (802) 828-3171
FAX: (802) 828-3187
http://www.ago.vermont.gov

July 28, 2017

Donna Waters, COM
Washington Superior Court
65 State Street
Montpelier, VT 05602

Hand Delivered

Re: *State of Vermont v. David Bushey*

Dear Ms. Waters:

Enclosed for filing with the Court on the above-referenced matter, please find the Assurance of Discontinuance. I would appreciate you returning the copy to me with your date stamp noted.

Thank you.

Sincerely yours,

My-Lanh S. Graves
Administrative Secretary

Enc.

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

In Re: DONNA AIKEN) CIVIL DIVISION
) Docket No. 674-11-17 Wncv

ASSURANCE OF DISCONTINUANCE

The State of Vermont, by and through Vermont Attorney General Thomas J. Donovan, Jr., and Donna Aiken ("Respondent"), hereby enter into this Assurance of Discontinuance ("AOD") pursuant to 9 V.S.A. § 2459.

Regulatory Framework

1. Lead-based paint in housing, the focus of the Vermont lead law, is a leading cause of childhood lead poisoning, which can result in adverse health effects, including decreases in IQ.
2. All paint in pre-1978 housing is presumed to be lead-based unless a certified inspector has determined that it is not lead-based. 18 V.S.A. § 1759(a).
3. All paint in rental target housing is "presumed to be lead-based unless a lead inspector or lead risk assessor has determined that it is not lead-based." 18 V.S.A. § 1760(a).
4. The lead law requires that essential maintenance practices ("EMPs") specified in 18 V.S.A. § 1759 be performed at all pre-1978 rental housing.
5. EMPs include, but are not limited to, installing window well inserts, visually inspecting properties at least annually for deteriorated paint, restoring surfaces to be free of deteriorated paint within 30 days after such paint has been visually identified

Office of the ATTORNEY GENERAL
109 State Street
Montpelier, VT 05609

or reported to the owner, and posting lead-based paint hazard information in a prominent place. 18 V.S.A. § 1759(a) (2), (4) and (7).

6. The EMP requirements also mandate that an owner of rental target housing file affidavits or compliance statements attesting to EMP performance with the Vermont Department of Health and with the owner's insurance carrier. 18 V.S.A. § 1759(b).
7. A violation of the lead law requirements may result in a maximum civil penalty of $10,000.00. 18 V.S.A. § 130(b)(6). Each day that a violation continues is a separate violation. 18 V.S.A. § 130(b)(6).
8. The Vermont Consumer Protection Act, 9 V.S.A Chapter 63, prohibits unfair and deceptive acts and practices, which includes the offering for rent, or the renting of, target housing that is noncompliant with the lead law.
9. Violations of the Consumer Protection Act are subject to a civil penalty of up to $10,000.00 per violation. 9 V.S.A. § 2458(b)(1). Each day that a violation continues is a separate violation.

Respondent's Rental Housing and Lead Compliance Practices

10. Respondent is the owner of a rental property at 11 Green Street in Bellows Falls, VT (4 units).
11. The property was constructed prior to 1978, and therefore, is pre-1978 "rental target housing" within the meaning of the Vermont lead law, 18 V.S.A. § 1751(23), and is subject to the requirements of 18 V.S.A. Chapter 38.
12. Respondent has in the past and continues presently to rent and offer for rent units in the property.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

13. On August 3, 2017, Respondent filed with the Vermont Department of Health an "EMP Rental Property Compliance Statement" for 11 Green Street.

14. The EMP Statement represented that Respondent performed EMPs at 11 Green Street on July 28, 2017.

15. The EMP Statement specifically certifies that Respondent:

    a. visually inspected exterior surfaces and outbuildings;

    b. stabilized exterior paint; and

    c. did not identify deteriorated paint exceeding 1 square foot on exterior surfaces of the buildings.

16. The EMP Statement was signed by Donna Aiken and certified that "all information provided on this form is true and accurate" and acknowledged that "providing false, incomplete or inaccurate information on this form is unlawful and is punishable by civil and criminal penalties pursuant to Vermont law."

17. On August 30, 2017, Vermont Department of Health staff inspected the exterior of 11 Green Street and documented (via photographs) deteriorated paint exceeding more than 1 square foot on the property's exterior surface.

18. Respondent admits the truth of the facts described in ¶¶ 10-16.

The State's Allegations

19. The Vermont Attorney General's Office alleges the following violations of the Consumer Protection Act and Lead Law:

    a. Submitting a false EMP compliance statement and inaccurately representing that the property was in compliance with the lead law.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

20. The State of Vermont alleges that the above behavior constitutes unfair and deceptive acts and practices under 9 V.S.A. § 2453.

Assurances and Relief

In lieu of instituting an action or proceeding against Respondent, the Attorney General and Respondent are willing to accept this AOD pursuant to 9 V.S.A. § 2459. Accordingly, the parties agree as follows:

21. Respondent shall fully and timely comply with the requirements of the Vermont lead law, 18 V.S.A., Chapter 38, as long as they maintain any ownership or property management interest in the property and in any other pre-1978 rental housing in which they currently have, or later acquire, an ownership or property management interest.

22. By May 31, 2018, all exterior EMP work of the property shall be completed in a lead-safe manner in accordance with 18 V.S.A. § 1760. If Respondent requires additional time to complete the work, Respondent will contact the Department of Health to request an extension of time agreement before the expiration of the above deadlines and provide a detailed justification for any extension. Any extension will be granted only for the exterior of the Property; all interior work must be completed by December 1, 2017.

23. Within one week of completion of the EMP work at the property described in the paragraph above, Respondent will file with the Vermont Department of Health, Respondent's insurance carrier and with the Office of the Attorney General, an updated and completed EMP compliance statement for the property, and will give a copy of the compliance statement to an adult in each rented unit of the property. The

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

copy for the Office of the Attorney General shall be sent to: Justin Kolber, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.

24. In the event Respondent wishes to rent a unit which becomes vacant in any of Respondent's pre-1978 rental housing before such housing is made EMP compliant, Respondent shall provide advance written notice of the intent to rent to the Office of the Attorney General at the address listed above. Respondent's advance written notice shall also: (1) verify that the interior of the specific unit to be rented is EMP compliant; (2) provide an update as to any remaining EMP work to be performed at the property, including the date by which the entire property will be EMP compliant. Otherwise, Respondent shall not rent, or offer for rent, any unit which becomes vacant in any of property owned or managed by Respondent that is not EMP compliant until such time as the EMP work is complete and the EMP compliance statement is distributed as described above.

25. Respondent shall pay the sum of $5,000 in civil penalties and costs for the filing of a false EMP compliance statement, as follows: (1) reduced amount of $500, based on demonstrated financial hardship, paid to the "State of Vermont" and sent to the following address: Justin E. Kolber, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609; and (2) $4,500 to be expended on lead hazard reduction improvements at the property.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

Other Terms

26. This AOD is binding on Respondent, however, sale of any pre-1978 rental property may not occur unless Respondent has complied with all obligations under this AOD,

or this AOD is amended in writing to transfer to the buyer or other transferee all remaining obligations.

27. Transfer of ownership of any of Respondent's pre-1978 rental property shall be consistent with Vermont law, including the provisions of 18 V.S.A. § 1767 specifically relating to the transfer of ownership of pre-1978 rental housing.
28. This AOD shall not affect marketability of title.
29. Nothing in this AOD in any way affects Respondent's other obligations under state, local, or federal law.
30. In addition to any other penalties or relief which might be appropriate under Vermont law, any future failure by Respondent to comply with the terms of this AOD shall be subject to a liquidated civil penalty paid to the State of Vermont in the amount of at least $5,000 and not more than $10,000.

SIGNATURES APPEAR ON NEXT PAGE

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

DATED at Montpelier, Vermont this 22nd day of November, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____

Justin E. Kolber
Assistant Attorney General
Office of the Attorney General
109 State Street
Montpelier, VT 05609
(802) 828-5620
justin.kolber@vermont.gov

DATED at Bellows Falls, Vermont this 19 day of November, 2017.

DONNA AIKEN

By: _____

Donna Aiken

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

STATE OF VERMONT

SUPERIOR COURT
Washington Unit

CIVIL DIVISION
Docket No. 325-6-16 Wncv

STATE OF VERMONT,
Plaintiff,

v.

FIRECO, LLC,
Defendant.

ORDER

CONSENT DECREE, ORDER, AND FINAL JUDGMENT

The Plaintiff, State of Vermont, by and through Attorney General Thomas J. Donovan, Jr., filed a Complaint in the above-captioned matter alleging violations of certain state laws by the Defendant, FireCo, LLC ("FireCo"). Defendant has answered said Complaint denying the allegations and asserting numerous affirmative defenses. In order to resolve the matter on a compromise basis, prior to any ruling by the Court, the parties further stipulate and agree as follows:

BACKGROUND

1. The State of Vermont is the Plaintiff in this case and is represented by the Attorney General of the State of Vermont.

2. Defendant FireCo is a for-profit corporation that is incorporated under the laws of the State of Tennessee, with its principal place of business located at 150B Cude Lane, Madison, TN 37115.

3. Between 2006 and 2013, FireCo solicited contributions as a paid fundraiser and was paid by the Professional Fire Fighters of Vermont ("PFFV"), a "charitable organization" as that term is defined in 9 V.S.A. § 2471(2).

4. The fundraising campaigns conducted by FireCo included the opportunity to attend a concert performed by entertainers in various venues throughout the state. Donors who agreed to contribute $25 or more received vouchers that were redeemable for admittance.

5. Pursuant to 9 V.S.A. §§ 2473(a) and 2477, FireCo filed notices of solicitation and financial reports with the Office of the Attorney General identifying the following 14 fundraising campaigns it has undertaken on behalf of PFFV since November 2006:

Campaign ID No.	**Start Date**	**End Date**
10080	11/10/2006	5/12/2007
10166	5/4/2007	11/18/2007
10300	11/9/2007	5/7/2008
10460	5/9/2008	11/15/2008
10571	11/7/2008	5/16/2009
10689	5/8/2009	11/14/2009
10802	11/6/2009	5/15/2010
10969	5/7/2010	11/13/2010
11132	11/5/2010	5/14/2011
11354	5/8/2011	11/12/2011
11522	11/4/2011	5/12/2012
11694	5/4/2012	11/10/2012
11849	11/2/2012	5/11/2013
12030	5/3/2013	11/9/2013

6. In the case of each fundraising campaign it has undertaken as a paid fundraiser on behalf of PFFV since 2006 ("each campaign"), FireCo has solicited contributions by telephone communication with potential donors, as well as by written solicitation.

7. In connection with each campaign, FireCo's written disclosure regarding the percentages of contributions to be paid to the charitable organization and paid fundraiser substantively met the requirements of Vermont law, but there was a technical violation of the State's rules in that the disclosure was not put in the physical location in the solicitation materials as required by CP 119.07(c).

8. In connection with Campaign ID # 10300, 10460, 10571, 10689, 10802, 10969, 11132, 11354, 11522, 11694, and 11849, the State alleges that FireCo failed to file the closing statement required by 9 V.S.A. § 2476(c). FireCo admits to a technical violation of this provision occurred in that "closing statements" were not sent, but FireCo has asserted that all of the information necessary in a "closing statement" was already in the possession of the PFFV.

9. Except where denied here and above, FireCo admits the truth of the other facts set forth in the Background section.

10. The Attorney General alleges that the above conduct violated 9 V.S.A. § § 2453, 2475(e)(2), 2476(c) and CP Rule 119.07. FireCo has not admitted any violation of any Vermont consumer protection law or rule pursuant to Title 9, except the technical violations referred to above, and enters into this Consent Decree and Final Judgment as a compromise settlement of a disputed claim.

REMEDIES

11. Nothing herein shall prejudice the right of FireCo to re-register as a paid fundraiser in Vermont.

12. In any future solicitation campaign in Vermont, FireCo, when acting as a paid fundraiser, will comply with all provisions of the Charitable Solicitations Law and

Rule CP 119, including (1) the requirements under 9 V.S.A. § 2475(e)(2) and Rule CP 119.07(c) with respect to making written disclosures to potential contributors with each solicitation; and (2) the requirement under 9 V.S.A. § 2476(c) with respect to filing a closing statement with the charitable organization.

13. Commencing with the execution of this Consent Decree, Order, and Final Judgment ("Consent Judgment") and continuing for three successive fundraising campaigns undertaken by FireCo as a paid fundraiser in Vermont on behalf of any charitable organization, FireCo shall:

(a) designate an individual to serve as FireCo's Compliance Officer, who shall supervise all individuals engaged in charitable fundraising activities on behalf of FireCo and ensure that all such individuals are fully compliant with the Charitable Solicitations Law and Rule CP 119. FireCo shall promptly implement policies and procedures and train all officers, managers, and employees, as appropriate to their respective roles and responsibilities, to ensure compliance with Vermont law. The Compliance Officer and all FireCo officers and managers shall be provided with a copy of this Consent Judgment and shall be required to review it and be familiar with its terms. FireCo shall, 15 days in advance of the commencement of a future solicitation campaign in Vermont, provide to the Attorney General's Office, in writing, the identity of its Compliance Officer, as well as a phone number and email address for that individual;

(b) submit to the Attorney General's Office, not less than 15 days prior to the commencement of each fundraising campaign undertaken in Vermont on behalf of any charitable cause, a certification that a Vermont attorney has reviewed a copy of

all written materials that FireCo will or may employ in connection with any oral solicitation during the course of the fundraising campaign, including all telephone scripts, rebuttals, and prepared responses in anticipation of possible questions or comments from potential contributors;

(c) make and retain audio recordings of all telephone solicitations or other oral communications with a potential contributor; and

(d) submit to the Attorney General's Office, in accordance with the filing deadline in 9 V.S.A. § 2476(c), a copy of each closing statement for each fundraising campaign containing all the information required by § 2476(c), and shall certify that it has provided each closing statement in a timely manner to the charitable organization on whose behalf FireCo has engaged in charitable solicitation.

(e) all such requirements shall remain in full force and effect for a period of three years from the date of this Order pertaining to FireCo's future conduct in the State of Vermont when acting as a paid fundraiser as that term is defined by the statute.

14. FireCo shall retain for a period of three years from the end of each charitable solicitation campaign:

(a) all written materials used in connection with soliciting charitable contributions from Vermont residents, including all written solicitation materials and all telephone scripts, rebuttals, and other written materials used in connection with oral solicitation;

(b) all records of communications that have been made or received in connection with soliciting charitable contributions from Vermont residents, including but not limited to all audio recordings and electronic communications;

(c) all documents supporting any factual representation made orally or in writing during the course of any charitable solicitation; and

(d) all records and materials that document the representations made in FireCo's financial reports filed pursuant to 9 V.S.A. § 2477 and FireCo's closing statements filed pursuant to 9 V.S.A. § 2476(c), including but not limited to records that document the contribution made by any individual or entity, bills and invoices, records of payments made and payments received by FireCo or the charitable organization, demands for payment, ledgers, accountings, reconciliations, and worksheets and calculations generated in the course of preparing the financial report or the closing statement.

15. Within thirty (30) days of signing this Consent Judgment, FireCo shall:

a. Show proof that a voluntary donation of twenty thousand dollars ($20,000) was made as a means of effectuating the donors' presumptive intent to the Vermont Community Foundation, located at 3 Court Street, Middlebury, Vermont, 05753, to be distributed in that organization's reasonable discretion to a charitable organization supporting Vermont firefighters. A copy of the check and transmittal letter shall be sent to the Assistant Attorney General identified in subparagraph (b), below.

b. Pay the sum of fifteen thousand dollars ($15,000) to the State of Vermont as an agreed upon payment for the State's fees and costs in connection with this matter. Payment shall be made either by wire transfer or in the form of a bank or cashier's check delivered to Assistant Attorney General Charity R. Clark, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.

16. If the Superior Court of the State of Vermont, Washington Unit enters an Order finding the Defendant to be in violation within three years of the date of this Order, then the parties agree that penalties to be assessed by the Court for each violative act shall be $10,000. Defendant shall pay all costs of any enforcement of this Consent Judgment.

17. This Court finds that the parties have agreed that technical violations were made pursuant to 9 V.S.A. § 2476(c) and CP 119.07(c).

18. This Court has jurisdiction over the subject matter of this action and the Defendant. Jurisdiction is retained by this Court over this Consent Judgment and the parties for the purposes of enabling any of the parties to apply to this Court at any time for orders and directions as may be necessary to carry out or construe this Consent Judgment, to modify any of its provisions, to enforce compliance, and to punish violations of its provisions.

19. This Consent Judgment shall be binding upon FireCo and its successors and assigns.

STIPULATION

Defendant FireCo, LLC acknowledges receipt of and voluntarily agrees to the terms of this Consent Judgment and waives any formal service requirements thereof.

DATED at _____, _____ this 10th day of July, 2017.

FireCo, LLC

By: Stanley R Taylor, President
Authorized Representative

ACCEPTED on behalf of the Attorney General:

DATED at Montpelier, Vermont this 10th day of July, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____

Charity R. Clark
Assistant Attorney General
Vermont Attorney General's Office
109 State Street
Montpelier, VT 05609
Tel. (802) 828-1422
charity.clark@vermont.gov

APPROVED AS TO FORM:

_____

Charity R. Clark
Assistant Attorney General
Office of the Attorney General
109 State Street
Montpelier, Vermont 05609

For the State of Vermont

_____

Kerin Stackpole, Esq.
Kristina Brines, Esq.
Paul Frank + Collins
One Church Street
P.O. Box 1307
Burlington, Vermont 05402-1307
For Defendant

_____

Errol Copilevitz, Esq.
Copilevitz & Canter, LLC
310 W. 20th Street, Suite 300
Kansas City, MO 64108
For Defendant

DECREE, ORDER, AND FINAL JUDGMENT

This consent decree is accepted and entered as a Decree, Order, and Final Judgment of this Court in the matter of State of Vermont v. FireCo, LLC, Docket No. 325-6-16 Wncv.

SO ORDERED.

DATED at Montpelier, Vermont this 11th day of July, 2017.

Mary Miles Teachout
Washington Superior Court Judge

7069659_5:12492-00001

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

STATE OF VERMONT Plaintiff, v. GENERAL MOTORS COMPANY, Defendant.	CIVIL DIVISION Docket No._____ AGREED CONSENT JUDGMENT ENTRY AND ORDER

FILED
2011 OCT 26 P 1:05
VT SUPERIOR COURT
WASHINGTON UNIT

Plaintiff, the State of Vermont, acting by and through Attorney General Thomas J. Donovan, Jr. has brought this action pursuant to 9 V.S.A. § 2451, *et seq.* of the Vermont Consumer Protection Act("CPA"), having filed a Complaint against General Motors Company ("GM").

Plaintiff and GM, by their counsel, have agreed to the entry of this Agreed Consent Judgment ("Consent Judgment") without trial or adjudication of any issue of fact or law and without admission by GM of any wrongdoing or admission of any of the violations of the Vermont Consumer Protection Act as alleged by Plaintiff.

Contemporaneous with the filing of this Consent Judgment, GM is entering into similar agreements with the Attorneys General of Alabama, Alaska, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Mississippi, 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, Virginia, Washington, West Virginia, Wisconsin, and Wyoming (hereinafter collectively referred to as "Attorneys General" or "Signatory Attorneys General").

1. PRELIMINARY STATEMENT

1.1 In 2014, an Attorneys General Multistate Working Group ("MSWG")—of which Vermont is a member—initiated an investigation (the "Investigation") into certain business practices of GM[1] concerning GM's issuance of the following Recalls: NHTSA Recall Nos. 14V047, 14V346, 14V355, 14V394, 14V400, 14V490, and 14V540.

1.2 The MSWG was led by a Multistate Executive Committee ("MSEC") comprised of Connecticut, Florida, Maryland, Michigan, New Jersey, Ohio, Pennsylvania, South Carolina, and Texas.

1.3 The Investigation was prompted by reports of unintended key rotation related and/or ignition switch-related Recalls in several models and model years of GM vehicles.

1.4 The Investigation focused on the "Covered Conduct," as that term is defined herein.

1.5 This Investigation was based upon, and has proceeded under, the Attorney General of the State of Vermont's authority to act on behalf of, and to protect, the people of Vermont against alleged harms to Consumers pursuant to 9 V.S.A. 2453.

1.6 On or about May 16, 2014, GM agreed to a Consent Order with NHTSA related to the NHTSA 14V047 Recall that included, among other provisions, certain improvements GM agreed to make to its Recall process and its handling of issues related to the safety of GM Motor Vehicles (the "NHTSA Consent Order").

---

[1] The Investigation sought information about events that preceded the bankruptcy of General Motors Corporation ("Old GM"). GM does not admit any wrongdoing or accept any liability for conduct allegedly involving or relating to the activities of Old GM. Nothing in this Consent Judgment is intended to imply or suggest that GM is responsible for any acts, conduct, or knowledge of Old GM, or that such acts, conduct, or knowledge, can be imputed to GM. Nor is anything in this Consent Judgment intended to alter, modify, expand, or otherwise affect any provision of the July 5, 2009 Sale Order issued by the U.S. Bankruptcy Court for the Southern District of New York, or the rights, protections, and responsibilities of GM under the Sale Order or pertinent law.

1.7 GM represents, and by entering into this Consent Judgment, the Attorneys General rely upon, that in compliance with the requirements set by NHTSA under the Federal Motor Vehicle Safety Act, GM does and shall timely notify GM Motor Vehicle owners of a known defect related to Motor Vehicle safety in GM Motor Vehicles.

1.8 On or about September 16, 2015, GM agreed to a Deferred Prosecution Agreement with the U.S. Department of Justice (the "DPA"). Pursuant to the DPA, the U.S. Department of Justice appointed a Monitor to assess GM's compliance with the DPA and to make recommendations for additional improvements that GM is required by the DPA to adopt unless it objects to a recommendation and the U.S. Department of Justice agrees that adoption of such recommendation is not required.

1.9 The Signatory Attorneys General recognize that GM has cooperated with the Investigation and has, prior to the Effective Date, voluntarily implemented improvements to its safety organization and to its safety processes.

1.10 The Parties have reached an amicable agreement resolving the issues in controversy and concluding the Investigation by filing/entering this Consent Judgment. The Parties agree that this Consent Judgment resolves the Signatory Attorneys' General claims and potential claims under their UDAP Laws as defined in Paragraph 5.27 and as set forth in Section 8 of this Consent Judgment.

NOW THEREFORE, upon the consent of the Parties hereto, IT IS HEREBY ORDERED, ADJUDGED AND DECREED AS FOLLOWS:

2. PARTIES

2.1 Plaintiff is the State of Vermont. "Attorney General" shall refer to the Attorney General of the State of Vermont.

2.2 Defendant is General Motors Company or "GM," which is headquartered in Detroit, Michigan.

3. JURISDICTION

3.1 Pursuant to 9 V.S.A. § 2458, jurisdiction of this Court over the subject matter and over the Defendant for the purpose of entering into and enforcing this Consent Judgment is admitted. Jurisdiction is retained by this Court for the purpose of enabling the Attorney General or the Defendant to apply for such further orders and directions as may be necessary or appropriate for the construction and modification of the injunctive provisions herein, or execution of this Consent Judgment, including enforcement of this Consent Judgment and punishment for any violation of this Consent Judgment. The Defendant waives any defect associated with service of Plaintiff's Complaint and this Consent Judgment and does not require issuance or service of a Summons.

4. VENUE

4.1 Pursuant to the provisions of 9 V.S.A. § 2458 venue as to all matters between the Parties relating to or arising out of this Consent Judgment shall lie exclusively in the Superior Court, Washington County, Vermont or other State Court of competent jurisdiction in the same district.

5. DEFINITIONS

In this Consent Judgment, the following words or terms shall have these meanings:

5.1 "Advertise," "Advertisement," or "Advertising" means any written, oral, or electronic statement, illustration, or depiction intended for Consumers and designed to create interest among Consumers in the purchase of, impart information about the attributes of, publicize the availability of, or effect the sale or use of, goods or services, whether the statement appears in a brochure, certification, newspaper, magazine, free-standing insert, marketing kit, leaflet, circular,

mailer, book insert, letter, catalogue, poster, chart, billboard, public-transit card, point-of-purchase display, package insert, package label, product instructions, electronic mail, website, mobile application, homepage, film, slide, radio, television, cable television, program-length commercial or "infomercial," or any other medium whether in print or electronic form.

5.2 "Affected Vehicles" means the vehicles included in the Investigation Recalls defined in Paragraph 5.14, below.

5.3 "Affiliates" means those individuals, corporations, partnerships, joint ventures, trusts, associations, or unincorporated associations specifically listed on Exhibit A and including Vehicle Acquisition Holdings, LLC, and NGMCO, Inc.

5.4 "Attorney General" or "Signatory Attorney General" means the Attorney General of the State of Vermont and/or the Office of the Attorney General of Vermont.

5.5 "Clear and Conspicuous" or "Clearly and Conspicuously" when referring to a statement or disclosure, means that such statement or disclosure is disclosed in such size, color, contrast, location, duration, and audibility that it is readily noticeable, readable, understandable, or, if applicable, capable of being heard. A statement may not contradict or be inconsistent with any other information with which it is presented. If a statement modifies, explains, or clarifies other information with which it is presented, it must be presented in proximity to the information it modifies, in a manner that is likely to be noticed, readable, and understandable, and it must not be obscured in any manner. Audio disclosures shall be delivered in a volume and cadence sufficient for a Consumer to hear and comprehend. Visual disclosures shall be of a size and shade and appear on the screen for a duration sufficient for a Consumer to read and comprehend. In a print Advertisement or promotional material, including, without limitation, point of sale display or brochure materials directed to Consumers, the disclosures shall be in a type, size, and location

sufficiently noticeable for a Consumer to read and comprehend, in a print that contrasts with the background against which it appears.

5.6 "Confidentiality Agreement" means the Confidentiality Agreement executed on or about June 29, 2015.

5.7 "Consent Judgment" refers to this document entitled Agreed Consent Judgment Entry and Order in the matter of State of State of Vermont v. General Motors Company.

5.8 "Consumer" means any person, a natural person, individual, governmental agency or entity, partnership, corporation, limited liability company or corporation, trust, estate, incorporated or unincorporated association, or any other legal or commercial entity, however organized, to whom GM directly or indirectly offered its vehicles, products, or services for sale or lease.

5.9 "Covered Conduct" means the engineering, manufacturing, marketing, sales, and maintenance of the Affected Vehicles arising from the unintended key rotation-related and/or ignition-switch-related Recalls including (1) when Old GM or GM became aware of an ignition switch problem and whether Old GM or GM made timely disclosures of known defects to Consumers and regulators; (2) whether Old GM or GM misrepresented, expressly, impliedly or by omission, the safety, reliability or resale value of the Affected Vehicles to Consumers and regulators; (3) whether Old GM or GM engaged in deceptive Advertising of the Affected Vehicles; and (4) whether Old GM or GM engaged in the resale or offering for resale of any Affected Vehicles with alleged ignition switch safety problems.

5.10 "Effective Date" means the date on which this Consent Judgment has been signed by both Parties and entered as an order by the Court.

5.11 "Fantasy Advertising" means Advertising that uses special effects or fictional characters.

5.12 "GM" means General Motors Company and its present parents, subsidiaries (whether or not wholly owned), and Affiliates. For the avoidance of doubt, undertakings by GM in this Consent Judgment do not include or extend to GM dealers or distributors.

5.13 For purposes of this Consent Judgment only, "Ignition Switch" refers to any defective ignition switch in any of the Affected Vehicles that is the subject of any of the Recalls that are the subject of the multistate Investigation.

5.14 "Investigation Recalls" means NHTSA Recall Nos. 14V047, 14V346, 14V355, 14V394, 14V400, 14V490, and 14V540.

5.15 "Monitor" means the Monitor appointed by the U.S. Department of Justice, pursuant to the DPA, as referenced in Paragraph 1.8.

5.16 "Motor Vehicle," as used herein, means a self-propelled vehicle manufactured for use on public streets, roads, or highways, but not on railroads.

5.17 "NHTSA" means the National Highway Traffic Safety Administration. If any obligations, duties, or the jurisdiction of NHTSA should be transferred, consolidated, or merged with the obligations, duties, or jurisdiction of any other federal governmental agency or entity during the term of this Consent Judgment, then all references to "NHTSA" in this Consent Judgment shall apply to that other governmental agency or entity.

5.18 "Recall 14V047" means NHTSA Recall No. 14V047, which includes these Motor Vehicles: Model Year ("MY") 2005-2010 Chevrolet Cobalt, MY 2006-2011 Chevrolet HHR, MY 2005-2006 Pontiac Pursuit, MY 2006-2010 Pontiac Solstice, MY 2007-2010 Pontiac G5, MY 2003-2007 Saturn Ion, and MY 2007-2010 Saturn Sky.

5.19 "Recall 14V346" means NHTSA Recall No. 14V346, which includes these Motor Vehicles: MY 2010-2014 Chevrolet Camaro.

5.20 "Recall 14V355" means NHTSA Recall No. 14V355, which includes these Motor Vehicles: MY 2005-2009 Buick LaCrosse, MY 2006-2011 Buick Lucerne, MY 2000-2005 Cadillac DeVille, MY 2006-2011 Cadillac DTS, MY 2006-2014 Chevrolet Impala, and MY 2006-2007 Chevrolet Monte Carlo.

5.21 "Recall 14V394" means NHTSA Recall No. 14V394, which includes these Motor Vehicles: MY 2003-2014 Cadillac CTS and MY 2004-2006 Cadillac SRX.

5.22 "Recall 14V400" means NHTSA Recall No. 14V400, which includes these Motor Vehicles: MY 2000-2005 Chevrolet Impala, MY 1997-2003 Chevrolet Malibu, MY 2004-2005 Chevrolet Malibu Classic, MY 2000-2005 Chevrolet Monte Carlo, MY 1999-2004 Oldsmobile Alero, MY 1998-2002 Oldsmobile Intrigue, MY 1999-2005 Pontiac Grand Am, and MY 2004-2008 Pontiac Grand Prix.

5.23 "Recall 14V490" means NHTSA Recall No. 14V490, which includes the Motor Vehicle MY 2002-2004 Saturn Vue.

5.24 "Recall 14V540" means NHTSA Recall No. 14V540, which includes these Motor Vehicles: MY 2011-2013 Chevrolet Caprice and MY 2008-2009 Pontiac G8.

5.25 "Recall" or "Recalls" means a Motor Vehicle manufacturer's field action to remedy a safety-related defect or non-compliance pursuant to the Federal Motor Vehicle Safety Act, 49 U.S.C. §§ 30116-30120.

5.26 "Represent," "Representation," or "Representations" shall mean to communicate through certifications, claims, statements, questions, conduct, graphics, symbols, lettering,

formats, devices, language, documents, messages, or any other manner or means by which meaning might be conveyed.

5.27 "UDAP Laws" means all applicable consumer protection and unfair trade and deceptive acts and practices laws, including, without limitation, 9 V.S.A. 2451, *et seq.* , as well as common law and equitable claims.

6. CONDUCT PROVISIONS

6.1 For the avoidance of doubt, the Conduct Provisions in this Section shall apply exclusively to Motor Vehicles sold in the United States, and the obligations shall extend and relate solely to GM's conduct with respect to such Motor Vehicles.

6.2 GM, in connection with the marketing or Advertising of certified pre-owned Motor Vehicles shall not, in any manner, expressly or by implication:

6.2.1 Represent that certified pre-owned Motor Vehicles that GM Advertises are safe, have been repaired for safety issues, or have been subject to a rigorous inspection, unless the certified pre-owned Motor Vehicles are, based on dealer reports to GM, either not subject to any open Recalls relating to safety or repaired pursuant to such a Recall, and the Representation is otherwise not misleading. As provided in Paragraph 6.9, GM will continue to instruct its dealers that certified pre-owned Motor Vehicles shall not be certified or delivered to a customer until all Recall repairs have been completed.

6.2.2 Misrepresent the following:

6.2.2.1 Whether there is or is not an open Recall for safety issues on any certified pre-owned Motor Vehicle;

6.2.2.2 Whether GM, or GM dealers to GM's knowledge, have repaired certified pre-owned Motor Vehicles for open safety Recalls; and

6.2.2.3 Any other material fact about the safety of the certified pre-owned Motor Vehicle GM Advertises for sale.

6.3 For a reasonable time after announcement of a Recall, in order to allow GM sufficient time to administratively and promptly modify its offering or Advertising to comply with Paragraph 6.2 of this Consent Judgment, GM will not be held in violation of Paragraph 6.2 of this Consent Judgment. In recognition that the Recall repairs and the certification is done by GM's dealers, GM may rely on its dealers' reported certification of a Motor Vehicle in its Advertising and marketing materials pursuant to this Consent Judgment.

6.4 GM shall comply with Vermont's UDAP Laws that apply to GM and the Motor Vehicles it manufactures, markets, and sells in the United States.

6.5 Notice to Consumers.

6.5.1 GM will maintain a Vehicle Safety Owner Engagement Team (or its functional equivalent), which uses data analytics and customer research to analyze and, where appropriate in GM's discretion, develop and execute communications and outreach tactics to enhance Recall awareness by impacted customers in the U.S.

6.5.2 Within 60 days after one year after the Effective Date of this Consent Judgment, GM will provide the Signatory Attorneys General with a report that summarizes GM's activities relative to Paragraph 6.5.1 above.

6.6 Advertising.

6.6.1 With respect to Advertisements in Vermont concerning the product safety of GM Motor Vehicles, GM will not engage in misleading or false Advertising in violation of the CPA. When determining whether a particular Advertisement complies with the provisions in Section 6.6, the entire Advertisement shall be considered, including the context of the particular

depiction or phrase(s) at issue, any limitations, warnings, or disclosures in the Advertisement, and any limitations, warnings, or disclosures in the Motor Vehicle's owner's manual. Nothing herein shall preclude GM from (a) demonstrating the ordinary use of vehicle components, systems, or features, (b) demonstrating the performance of safety features, (c) depicting a Motor Vehicle being driven by a professional driver on a closed course, provided that any necessary and appropriate disclosures are Clearly and Conspicuously disclosed in the Advertisement, or (d) using Fantasy Advertising.

6.6.2 GM shall not Represent that a Motor Vehicle is "safe," "safest," "safer," or use a term or phrase of similar superlative or comparative meaning regarding safety, unless they have complied with those Federal Motor Vehicle Safety standards applicable to the Motor Vehicle at issue, and, if necessary, GM Clearly and Conspicuously discloses the information necessary to place the Representation in an accurate context, including by way of example: (a) the Motor Vehicle for which the claim is made; and (b) the design, feature, equipment or aspect of performance for which the claim is being made. The mere fact of a subsequent safety Recall of a Motor Vehicle by itself does not render a prior Advertisement of that Motor Vehicle misleading or otherwise state a violation of this Consent Judgment.

6.6.3 Notwithstanding Paragraph 6.6.2, GM may (a) make truthful Representations about the receipt of awards, ratings, or rankings from third parties (*e.g.*, NHTSA's New Car Assessment Program, J.D. Power & Associates, or the Insurance Institute for Highway Safety), including those relating to safety; (b) make truthful Representations about any Motor Vehicle and/or its systems and components which a Consumer should reasonably understand are statements of opinion or statements not easily and objectively verifiable as factually correct or incorrect; or (c) make truthful Representations that a Motor Vehicle has specific safety features.

6.7 Safety-Related Organizational Restructuring and Data Analytics.

6.7.1 GM will maintain a Global Vehicle Safety organization (or its functional equivalent) to identify and investigate issues related to the safety of GM Motor Vehicles.

6.7.2 GM will maintain a Global Product Integrity organization (or its functional equivalent). Among its other functions, the Global Product Integrity organization will establish processes to identify and resolve potential safety issues in the design of GM Motor Vehicles using Design for Failure Mode and Effects Analysis (or its functional equivalent) and/or other strategies selected by GM to achieve the same or similar results.

6.7.3 GM will maintain a Safety and Field Action Decision Authority (or its functional equivalent) responsible for making decisions with respect to Recalls of GM Motor Vehicles sold in the U.S.

6.7.4 GM will use advanced data analytics to identify, review, and analyze product anomalies and events in support of the Motor Vehicle safety field investigation process.

6.8 Internal Reporting of Safety Issues.

6.8.1 GM will establish or maintain a "Speak Up for Safety" program (or its functional equivalent) for its employees and GM dealer employees to report safety-related issues concerning GM Motor Vehicles.

6.8.2 GM will require its U.S. salaried employees, as appropriate, to confirm annually that they have reported any issues related to the safety of GM Motor Vehicles to the "Speak Up for Safety" program (or its functional equivalent) or to appropriate GM personnel consistent with GM's policies.

6.8.3 GM will establish or maintain a non-retaliation policy to protect employees who report an issue related to the safety of GM Motor Vehicles, and GM will not

retaliate or tolerate retaliation in any form against an employee because that employee reports an issue related to the safety of GM Motor Vehicles.

6.9 Certified Pre-Owned Vehicles.

6.9.1 GM will instruct its dealers that (i) all applicable Recall repairs must be completed, and reflected as such in GM's systems, before any GM Motor Vehicle sold in the U.S. and included in such Recall is eligible for certification, and (ii) if there is a Recall on any Certified Pre-Owned GM Motor Vehicle sold in the U.S., the required remedy or repair must be completed before such Motor Vehicle is delivered to a customer.

6.10 Motor Vehicle Parts.

6.10.1 GM will establish or maintain appropriate processes and/or policies to determine whether a change in a part for a GM Motor Vehicle sold in the U.S. affects the part's "Fit, Form, or Function," such that the part number should be changed.

6.10.2 GM will train employees whose responsibilities include evaluating whether a part change affects the part's "Fit, Form, or Function" to follow the processes that GM will establish and maintain per Paragraph 6.10.1.

6.11 Consumer Complaint Resolution

6.11.1 Within 30 days of the Effective Date, GM shall appoint a person or persons to act as a direct contact for the Signatory Attorney General's office for the resolution of Consumer complaints arising from the subject matter of the Covered Conduct. GM shall provide the Signatory Attorney General's office with the name(s), title(s), address(es), telephone number(s), facsimile number(s), and electronic mail address(es) of the person(s) designated, within 30 days of the Effective Date.

7. PAYMENT TO THE STATES

7.1 Within 30 days of the Effective Date of the Vermont Consent Judgment, GM shall pay One Hundred Twenty Million Dollars ($120,000,000.00) total, to be divided and paid by GM directly to each Signatory Attorney General of the MSWG in an amount to be designated in writing by and in the sole discretion of the MSEC. Of that amount, Vermont shall receive One Million, Sixty-Six Thousand, Four Hundred Eight-One Dollars and Twelve Cents ($1,066,481.12). The MSEC will provide GM with instructions for the payments to be distributed to each Signatory Attorney General under this Paragraph. Said payment shall be used for such purposes that may include, but are not limited to, attorneys' fees and other costs incurred in pursuing this Investigation, future public protection and education purposes, a consumer protection enforcement fund, or other purposes, including without limitation future consumer protection enforcement, consumer education, litigation funds, local consumer aid funds, public protection or consumer protection purposes or other purposes as allowed by state law at the sole discretion of each Signatory Attorney General, and in Vermont, pursuant to the Constitution of the State of Vermont, Ch. II § 27, and 32 V.S.A. § 462. GM shall have no property right, interest, claim, control over, or title to any monies paid by GM to the MSWG after the payment is made by GM under this Consent Judgment. The parties acknowledge that the payment described herein is not a fine, penalty, or payment in lieu thereof.

8. RELEASE

8.1 Upon full and complete payment of the amount(s) designated in Section 7, above, the Attorney General of the State of Vermont releases and forever discharges to the fullest extent possible that the Attorney General is authorized under the law, (i) GM and its present and former parents, subsidiaries (whether or not wholly owned), and Affiliates (including but not limited to Vehicle Acquisition Holdings, LLC, and NGMCO, Inc.), and (ii) the respective divisions,

organizational units, officers, directors, employees, agents, representatives, and in-house attorneys of those entities in Section (i) of this Paragraph (the "Released Parties") from the following: all civil claims (including claims for diminution in value), demands, causes of action, damages, equitable claims, injunctive relief, restitution, fines, costs, attorneys' fees and penalties, arising from the subject matter of the Covered Conduct, that the Vermont Attorney General, whether directly, indirectly, representatively, derivatively, in their sovereign enforcement capacity, or as *parens patriae* on behalf of state citizens or in any other capacity, could have asserted, before or as of the Effective Date, against the Released Parties under all UDAP Laws (collectively, the "Released Claims").

8.2 Notwithstanding any term of this Consent Judgment, the following do not comprise Released Claims:

(A) Private rights of action;

(B) Claims of environmental or tax liability;

(C) Criminal liability;

(D) Claims for actual physical damage to real or personal property;

(E) Claims alleging violations of state or federal securities laws;

(F) Claims alleging violations of state or federal antitrust laws;

(G) Any obligations created under this Consent Judgment;

(H) Any other civil or administrative liability that any person or entity, including the Released Parties, has or may have to the State of Vermont and any subdivision thereof, not expressly covered by the release in Paragraph 8.1 above; and

(I) Any claims, other than claims under the UDAP Laws, related to the Covered Conduct.

9. ENFORCEMENT

9.1 For a period of five years after the Effective Date, for the purpose of resolving disputes with respect to compliance with this Consent Judgment, duly authorized representatives of the Office of the Attorney General of the State of Vermont shall, if they believe that GM has engaged in a practice that violates any provision of this Consent Judgment, notify GM in writing of the Attorney General's belief that a violation has occurred. The Attorney General's notice shall include:

9.1.1 the specific basis for the belief;

9.1.2 the provision of the Consent Judgment that the practice appears to violate; and

9.1.3 a date by which GM must respond to the notification, provided, however, that the response date shall be at least 60 days after the date of notification.

9.2 Upon receipt of written notice, GM shall provide a written response to the Attorney General either explaining why GM believes that it is in compliance with this Consent Judgment or explaining how the alleged violation occurred and how GM intends to address it. Specifically when explaining how the alleged violation occurred, GM may offer and the Attorney General may, but is not required to, consider whether the alleged violation resulted from an honest mistake or inadvertent error.

9.3 In the event that GM's response to the written notice does not address the Attorney General's concerns, the Attorney General may assert that GM has violated this Consent Judgment in a separate civil action to enforce this Consent Judgment, or seek any other relief afforded by law for such violation(s), only after providing GM with at least 60 days to respond to the

notification as set forth in Paragraph 9.1 above. However, such Attorney General may take any action authorized by state or federal law without prior notice, except where such notice is required under state law, where the Attorney General reasonably concludes that, because of a specific practice, a threat to the health or safety of the public requires immediate action. Nothing in this paragraph shall be interpreted to create for the Attorney General new authority or right to take action that does not exist already under state or federal law, or to limit or remove the rights of GM under existing law to object to such action or otherwise to respond appropriately.

9.4 Nothing in this Section shall be construed to limit the Attorney General's authority provided under the Vermont Consumer Protection Act.

9.5 It is the Parties' intent that nothing in this Consent Judgment shall create a conflict with (i) federal, state, or local law applicable to GM, (ii) any provision of the NHTSA Consent Order or other orders or instructions issued by NHTSA, (iii) any provision of the DPA, (iv) any recommendation made by the Monitor and adopted by GM pursuant to the DPA, or (v) any provision of the December 8, 2016 Decision and Order and the related Consent Agreement with the Federal Trade Commission ("FTC Order"). The Parties agree that the requirements of law, or the applicable provisions of the DPA, FTC Order, or NHTSA Consent Order, or the applicable recommendations made by the Monitor and adopted by GM, shall take precedence over the requirements of this Consent Judgment.

9.6 In the event that GM believes such a conflict exists, GM must notify the Attorney General of the alleged conflict, stating with specificity the provision of this Consent Judgment they believe conflicts with the item(s) outlined in Paragraph 9.5 (i)-(v) above. The Attorney General shall respond to GM's notification of alleged conflict within 30 days. In the interim, GM shall continue to comply with the terms of this Consent Judgment to the extent possible.

10. NOTICES UNDER THIS CONSENT JUDGMENT

10.1 Any notices required to be sent to the Attorney General or to GM under this Consent Judgment shall be sent by certified mail, return-receipt requested. The documents shall be sent to the following addresses:

For the Attorney General of Vermont:

Jill S. Abrams, Esq.
Director, Consumer Division
Vermont Attorney General's Office
109 State Street
Montpelier, VT 05609

For GM:

Craig Glidden, Esq.
Executive Vice President, Legal and Public Policy and General Counsel
General Motors Co.
300 Renaissance Center
Detroit, MI 48226

Any party may change its designated notice recipient(s) by written notice to the other party.

11. GENERAL PROVISIONS

11.1 This Consent Judgment Represents the full and complete terms of the Parties' settlement.

11.2 This Consent Judgment shall be binding upon the Parties and their successors and assigns. In no event shall assignment of any right, power, or authority under this Consent Judgment void a duty to comply with this Consent Judgment.

11.3 Paragraphs 6.3, 6.5, 6.6.2, 6.6.3, 6.7, 6.8 and 6.11 of this Consent Judgment will expire on Effective Date plus five years. Paragraphs 6.2, 6.6.1, 6.9 and 6.10 of this Consent Judgment will expire on Effective Date plus ten years. These expirations are contingent upon GM not having been adjudged by a court in any MSWG state to have violated any provision of Section 6 of any MSWG Consent Judgment with respect to any act or omission by GM related to the

Covered Conduct. If, prior to Effective Date plus five years, GM is adjudged by a court in any MSWG state to have violated any provision of Section 6 of any MSWG Consent Judgment with respect to any act or omission by GM related to the Covered Conduct, GM shall continue to be subject to Paragraphs 6.3, 6.5, 6.6.2, 6.6.3, 6.7, 6.8 and 6.11 of this Consent Judgment until Effective Date plus seven years in all MSWG states. If, prior to Effective Date plus ten years, GM is adjudged by a court to have violated any provision of Section 6 of any MSWG Consent Judgment with respect to any act or omission by GM related to the Covered Conduct, GM shall continue to be subject to Paragraphs 6.2, 6.6.1, 6.9 and 6.10 of this Consent Judgment until Effective Date plus twelve years in all MSWG states. This Paragraph is in addition to all other remedies available to the Attorney General in law and equity.

11.4 Nothing in this Consent Judgment shall be construed to waive, limit, or expand any claim of sovereign immunity the State of Vermont may have in any action or proceeding.

11.5 Any failure of the Attorney General or GM to exercise its rights under this Consent Judgment shall not constitute a waiver of its rights.

11.6 Unless otherwise prohibited by law, any signatures by the Parties required for entry of this Consent Judgment may be executed in counterparts and by different signatories on separate counterparts, each of which shall be deemed an original, but all of which shall together be one and the same Consent Judgment. One or more counterparts of this Consent Judgment may be delivered by facsimile or electronic transmission with the intent that it or they shall constitute an original counterpart hereof.

11.7 Nothing in this Consent Judgment shall be construed to create, waive, or limit any private right of action.

11.8 GM is entering into this Judgment solely for the purpose of settlement, and nothing contained herein may be taken as or construed to be an admission, concession, finding, or conclusion of any violation of law, rule, or regulation, or of any other matter of fact or law, or of any liability or wrongdoing, all of which GM expressly denies. This Consent Judgment is not intended to constitute evidence or precedent of any kind except in any action or proceeding by one of the Parties (a) to enforce, rescind, or otherwise implement or affirm any or all of the terms of this Consent Judgment, or (b) to support a defense of res judicata, collateral estoppel, release, or other theory of claim preclusion, issue preclusion, or similar defense. The Released Parties' agreement to entry of this Consent Judgment is not an admission of liability. Nothing in this Consent Judgment affects the Released Parties' right to take or adopt any legal or factual position or defense in any other litigation or proceeding, or to cite or enforce the terms of the Release in Section 8.

11.9 The Attorney General of the State of Vermont, for the consideration set forth in this Consent Judgment, hereby agrees and covenants not to sue Motors Liquidation Company, General Motors Corporation, Motors Liquidation Company GUC Trust, Motors Liquidation Company Avoidance Action Trust, or any other trust established by the Motors Liquidation Company bankruptcy plan to hold or pay liabilities of Motors Liquidation Company or General Motors Corporation for any and all civil claims (including claims for diminution in value), demands, causes of action, damages, equitable claims, injunctive relief, restitution, fines, costs, attorneys' fees and penalties, arising from the subject matter of the Covered Conduct that the Attorney General is authorized under the law to bring and which the Attorney General could have asserted, before or as of the Effective Date, against the entities named in this covenant not to sue under all UDAP laws. This paragraph and covenant is limited, to the extent applicable, by

Paragraph 8.2 of this Consent Judgment. This covenant not to sue includes the agreement by the Attorney General of the State of Vermont not to file a claim or seek any payment related to violations of all UDAP Laws related to the Covered Conduct in the bankruptcy case entitled *In re Motors Liquidation Company, et al.*, Case No. 09-50026 (MG) (Bankr. S.D.N.Y.).

11.10 GM waives any claim for fees, costs, or expenses incurred before the entry of this Consent Judgment against the Signatory Attorney General, or against any of his agents or employees related in any way to this Consent Judgment, whether arising under common law or under the terms of any statute. Likewise, except as otherwise provided in this Consent Judgment, the Signatory Attorney General waives any claims for fees, costs, or expenses incurred before the entry of this Consent Judgment against GM related in any way to this Consent Judgment, whether arising under common law or under the terms of any statute. For these purposes, GM and the Signatory Attorney General each agree that they are not the prevailing party in this action because the Parties have reached a good faith settlement. GM and the Signatory Attorney General further waive any other right to challenge or contest the validity of this Consent Judgment.

11.11 GM further agrees to execute and deliver such authorizations, documents, and instruments as are required under the various judicial procedures for acceptance of this Consent Judgment in the jurisdiction in which it is being filed.

12. COMPLIANCE WITH ALL LAWS

12.1 Nothing in this Consent Judgment shall be construed as relieving GM of its obligations to comply with all state and federal laws, regulations, or rules, or as granting GM permission to engage in any acts or practices prohibited by such law, regulation, or rule.

12.2 The Plaintiff and the Defendant hereby stipulate and agree that the Order of this Court to be issued pursuant to this Consent Judgment shall act as an injunction.

13. REPRESENTATIONS AND WARRANTIES

13.1 GM warrants and Represents that it manufactured, sold, and distributed Motor Vehicles in the U.S. and further acknowledges that it is the proper party to this Consent Judgment and that General Motors Company is its true legal name.

13.2 The undersigned counsel for the State of Vermont warrants and Represents that he is fully authorized to execute this Consent Judgment on behalf of the Attorney General of the State of Vermont.

13.3 Counsel for GM shall provide a corporate resolution authorizing the execution of this Consent Judgment on its behalf and warrants and Represents that they are fully authorized to execute this Consent Judgment on behalf of GM.

13.4 Each of the Parties warrants and Represents that it negotiated the terms of this Consent Judgment in good faith.

13.5 Each of the Parties and signatories to this Consent Judgment warrants and Represents that it freely and voluntarily enters into this Consent Judgment without any degree of duress or compulsion.

13.6 GM shall not Represent or imply that the Signatory Attorneys General acquiesce in or approve of GM's past or current business practices, efforts to improve its practices, or any future practices that GM may adopt or consider adopting.

13.7 All Parties consent to the disclosure to the public of this Consent Judgment by GM and the Signatory Attorneys General.

13.8 Nothing in this Consent Judgment constitutes an agreement by the Attorneys General concerning the characterization of the payment to the Signatory Attorneys General, as outlined in Section 7, for the purpose of the Internal Revenue laws, Title 26 of the United States Code, or similar state tax codes or laws.

13.9 For purposes of construing this Consent Judgment, the Consent Judgment shall be deemed to have been drafted by all Parties and shall not, therefore, be construed against any Party for that reason in any dispute.

13.10 The Parties state that no promise of any kind or nature whatsoever (other than the written terms of this Consent Judgment) was made to them to induce them to enter into this Consent Judgment, and that they have entered into this Consent Judgment voluntarily.

13.11 This Consent Judgment constitutes the entire, complete, and integrated agreement between the Parties pertaining to the settlement and supersedes all prior and contemporaneous undertakings of the Parties in connection herewith except the Confidentiality Agreement. This Consent Judgment may not be modified or amended except by written consent of all the Parties.

14. PAYMENT OF FILING FEES

14.1 All filing fees associated with commencing this action and obtaining the Court's approval and entry of this Consent Judgment shall be borne by GM.

IT IS SO ORDERED, ADJUDGED AND DECREED.

This _____ day of _____, 2017.

_____

Superior Court Judge

JOINTLY APPROVED BY:

FOR THE VERMONT ATTORNEY GENERAL, THOMAS J. DONOVAN, JR.

October 23, 2017

Jill S. Abrams — **DATE**
Director, Consumer Protection Division
Vermont Attorney General's Office
109 State Street
Montpelier, VT 05609
(802) 828-1106
Jill.Abrams@vermont.gov

FOR DEFENDANT:

GENERAL MOTORS COMPANY

10/2/17

Ann Cathcart Chaplin — **DATE**
Deputy General Counsel, Litigation
General Motors LLC
300 Renaissance Center
Detroit, Michigan 48265

APPROVED AS TO FORM FOR ENTRY:

10/4/17

Thomas J. Perrelli — **DATE**
Jenner & Block LLP
1099 New York Avenue, N.W., Suite 900
Washington, D.C. 20001-4412
(202) 639-6004
TPerrelli@jenner.com

Counsel for General Motors Company

EXHIBIT A

Company Name	State or Sovereign Power of Incorporation
06 Ormskirk Limited	England and Wales Canada
2140879 Ontario Inc.	Ontario
2140879 Ontario Inc.	Canada
6153933 Canada Ltd.	Delaware
ACAR Leasing Ltd.	Delaware
ACF Investment Corp.	Germany
ACF Investment Corp.	Delaware
Adam Opel AG	Nevada
Adam Opel GmbH	Germany
Advance Motors Limited	England and Wales
AEye, Inc.	Delaware
AFS Management Corp.	Nevada
AFS SenSub Corp.	England
AFS SenSub Corp.	Nevada
Aftermarket (UK) Limited	Italy
Aftermarket (UK) Limited	England
Aftermarket Italia S.r.l. in liquidazione	Egypt
Aftermarket Italia S.r.l. in liquidazione	Italy
AL Mansour Automotive SAE	Delaware
Alphabet Energy, Inc.	Delaware
AmeriCredit Automobile Receivables Trust 2007- B-F	Delaware
AmeriCredit Automobile Receivables Trust 2007-D-F	Delaware
AmeriCredit Automobile Receivables Trust 2010-1	Delaware
AmeriCredit Automobile Receivables Trust 2010-2	Delaware
AmeriCredit Automobile Receivables Trust 2010-3	Delaware
AmeriCredit Automobile Receivables Trust 2010-4	Delaware
AmeriCredit Automobile Receivables Trust 2010-A	Delaware
AmeriCredit Automobile Receivables Trust 2010-B	Delaware
AmeriCredit Automobile Receivables Trust 2011-1	Delaware
AmeriCredit Automobile Receivables Trust 2011-2	Delaware
AmeriCredit Automobile Receivables Trust 2011-3	Delaware
AmeriCredit Automobile Receivables Trust 2011-4	Delaware
AmeriCredit Automobile Receivables Trust 2011-5	Delaware
AmeriCredit Automobile Receivables Trust 2012-1	Delaware
AmeriCredit Automobile Receivables Trust 2012-2	Delaware
AmeriCredit Automobile Receivables Trust 2012-3	Delaware
AmeriCredit Automobile Receivables Trust 2012-4	Delaware
AmeriCredit Automobile Receivables Trust 2012-5	Delaware
AmeriCredit Automobile Receivables Trust 2013-1	Delaware

Company Name	State or Sovereign Power of Incorporation
AmeriCredit Automobile Receivables Trust 2013-2	Delaware
AmeriCredit Automobile Receivables Trust 2013-3	Delaware
AmeriCredit Automobile Receivables Trust 2013-4	Delaware
AmeriCredit Automobile Receivables Trust 2013-5	Delaware
AmeriCredit Automobile Receivables Trust 2014-1	Delaware
AmeriCredit Automobile Receivables Trust 2014-2	Delaware
AmeriCredit Automobile Receivables Trust 2014-3	Delaware
AmeriCredit Automobile Receivables Trust 2014-3	Nevada
AmeriCredit Automobile Receivables Trust 2014-4	Delaware
AmeriCredit Automobile Receivables Trust 2015-1	Delaware
AmeriCredit Automobile Receivables Trust 2015-2	Delaware
AmeriCredit Automobile Receivables Trust 2015-3	Delaware
AmeriCredit Automobile Receivables Trust 2015-4	Delaware
AmeriCredit Automobile Receivables Trust 2016-1	Delaware
AmeriCredit Automobile Receivables Trust 2016-2	Delaware
AmeriCredit Automobile Receivables Trust 2016-3	Delaware
AmeriCredit Automobile Receivables Trust 2016-4	Delaware
AmeriCredit Automobile Receivables Trust 2017-1	Delaware
AmeriCredit Automobile Receivables Trust 2017-2	Delaware
AmeriCredit Automobile Receivables Trust 2017-3	Delaware
AmeriCredit Automobile Receivables Trust 2017-4	Delaware
AmeriCredit Consumer Loan Company, Inc.	Nevada
AmeriCredit Consumer Loan Company, Inc. AmeriCredit Financial Services, Inc.	Delaware
AmeriCredit Financial Services, Inc.	Delaware
AmeriCredit Funding Corp. XI	Delaware
AmeriCredit Syndicated Warehouse Trust	Delaware
Amherstburg Chevrolet Buick GMC (2016) Limited	
Andersen & Martini Auto A/S	Denmark
Andiamo Riverfront, LLC	Michigan
Annunciata Corporation	Delaware
APGO Trust	Delaware
Approach (UK) Limited	England and Wales
Argonaut Holdings LLC	Delaware
Atlantic Automobiles SAS	France
Auto Distribution Provenance SAS	France
Auto Fornebu AS	Norway
Auto Lease Finance Corporation	Cayman Islands
Auto Partners III, Inc.	Delaware
Autohaus G.V.O. GmbH	Germany
Autovision (Scotland) Limited	Scotland
Autozentrum West Köln GmbH	Germany

Company Name	State or Sovereign Power of Incorporation
Aviation Spectrum Resources Holdings, Incorporated	Delaware
Ballards of Watford Limited	England and Wales
Banco GMAC S.A.	Brazil
Baylis (Gloucester) Limited	England and Wales
Beerens O.C. NV	Belgium
Berse Road (No. 1) Limited	England
Berse Road (No. 2) Limited	England
Betula Cars S.L.	Spain
BilCirkeln Malmo AB	Sweden
Blackdown Motor Company Limited	England and Wales
Bochum Perspektive 2022 GmbH	Germany
BOCO (Proprietary) Limited	South Africa
Boco Trust	South Africa
Boden Brussels NV	Belgium
Brandish Limited	England and Wales
Bridge Motors (Banbury) Limited	England and Wales
Bridgewater Chevrolet, Inc.	Delaware
Britain Chevrolet, Inc.	Delaware
BS Auto Praha sro	Czech Republic
Cadillac Europe GmbH	Switzerland
Cadillac of Greenwich, Inc.	Delaware
Carve-Out Ownership Cooperative LLC	Delaware
Caterpillar Logistics SCS	Italy
Certified Security Solutions, Inc.	Oregon
Charles Hurst Motors Limited	Northern Ireland
Chevrolet Austria GmbH	Austria
Chevrolet Austria GmbH in Liqu.	Austria
Chevrolet Belgium NV	Belgium
Chevrolet Cadillac of Pawling, Inc.	Delaware
Chevrolet Central and Eastern Europe	Hungary
Chevrolet Deutschland GmbH	Germany
Chevrolet Espana, S.A.	Spain
Chevrolet Euro Parts Center B.V.	Netherlands
Chevrolet Europe GmbH	Switzerland
Chevrolet Finland Oy	Finland
Chevrolet France	France
Chevrolet Italia S.p.A.	Italy
Chevrolet Nederland B.V.	Netherlands
Chevrolet of Fairfield, Inc.	Delaware
Chevrolet of Novato, Inc.	Delaware
Chevrolet Otomotiv Ticaret Limited Sirketi	Turkey

Company Name	State or Sovereign Power of Incorporation
Chevrolet Poland Sp. z o.o.	Poland
Chevrolet Portugal, Lda.	Portugal
Chevrolet Sales (Thailand) Limited	Thailand
Chevrolet Sales India Private Ltd.	India
Chevrolet Sociedad Anonima de Ahorro para Fines Determinados	Argentina
Chevrolet Suisse S.A.	Switzerland
Chevrolet Sverige AB	Sweden
Chevrolet UK Limited Ltd	England
CHEVYPLAN S.A. Sociedad Administradora de Planes de Autofinanciamiento Comercial	Colombia
CHEVYPLAN, CA	Venezuela, Bolivarian Republic
Claro Automobiles SAS	France
Comercial	Colombia
Controladora General Motors, S.A. de C.V.	Mexico
Coskata, Inc.	Delaware
Countryside Chevrolet, Inc.	Delaware
Courtesy Buick-GMC, Inc.	Delaware
Crash Avoidance Metrics Partners LLC	Michigan
Crash Avoidance Metrics Partnerships	Michigan
Crosby Automotive Group, Inc.	Delaware
Curt Warner Chevrolet, Inc.	Delaware
Daniels Chevrolet, Inc.	Delaware
DCJ 1 LLC	Delaware
Dealership Liquidations, Inc.	Delaware
DeCuir Automotive Group, Inc.	Delaware
Delphi Energy and Engine Management Systems UK Overseas Corporation	Delaware
Delta ID Inc.	Delaware
DENICAR S.R.L.	Italy
Detroit Investment Fund, L.P.	Delaware
Diso Madrid S.1.r.	Spain
Diso Madrid S.L.	Spain
DMAX, Ltd.	Ohio
Doraville Bond Corporation	Delaware
Drive Motor Properties LLP	England and Wales
Drive Motor Retail Limited	England and Wales
E. Maulme C. A.	Brazil
Eden (GM) Limited	England and Wales
Elasto S.A.	Ecuador
Empower Energies, Inc.	Delaware
Enchi Corporation	Delaware
Englewood Chevrolet, Inc.	Delaware
Envia Systems, Inc.	Delaware

Company Name	State or Sovereign Power of Incorporation
F G Barnes (Maidstone) Limited	England and Wales
Fabrica Nacional de Autobuses Fanabus, S.A.	Venezuela, Bolivarian Republic
FAW Harbin Light Duty Vehicle Company Limited	China
FAW-GM Hongta Yunnan Automobile Manufacturing Company Limited	China
FAW-GM Light Duty Commercial Vehicle Co., Ltd.	China
Flinc GmbH	Germany
Fludicon GmbH	Germany
Fox Valley Buick-GMC, Inc.	Delaware
Fuel Cell System Manufacturing LLC	Delaware
G.M.A.C. Financiera de Colombia S.A. Compania de Financiamiento Comercial	Colombia
G.M.A.C.-Comercio e Aluguer de Veiculos, Lda.	Portugal
General International Insurance Services Limited	Bermuda
General International Limited	Bermuda
General Motors - Colmotores S.A.	Colombia
General Motors (China) Investment Company Limited	China
General Motors (Hong Kong) Company Limited	Hong Kong
General Motors (Thailand) Limited	Thailand
General Motors Advisory Services LLC	Uzbekistan
General Motors Africa and Middle East FZE	United Arab Emirates
General Motors Asia Pacific (Pte) Ltd.	Singapore
General Motors Asia Pacific Holdings, LLC	Delaware
General Motors Asia, Inc.	Delaware
General Motors Asset Management Corporation	Delaware
General Motors Australia Ltd.	Australia
General Motors Austria GmbH	Austria
General Motors Auto LLC	Russian Federation
General Motors Automobiles Philippines, Inc.	Philippines
General Motors Automotive Holdings, S.L.	Spain
General Motors Belgique Automobile NV	Belgium
General Motors Belgium N.V.	Belgium
General Motors Brasil Holdings Ltda.	Brazil
General Motors Chile Industria Automotriz Limitada	Chile
General Motors China LLC	Delaware
General Motors China, Inc.	Delaware
General Motors CIS LLC	Russian Federation
General Motors Company	Delaware
General Motors Coordination Center BVBA	Belgium
General Motors Daewoo Auto and Technology CIS LLC	Russian Federation
General Motors de Argentina S.r.l.	Argentina
General Motors de Mexico, S. de R.L. de C.V.	Mexico
General Motors del Ecuador S.A.	Ecuador

Company Name	State or Sovereign Power of Incorporation
General Motors do Brasil Ltda.	Brazil
General Motors East Africa Limited	Kenya
General Motors Egypt, S,A.E.	Egypt
General Motors Espana, S.L.U.	Spain
General Motors Europe Holdings, S.L.U.	Spain
General Motors Europe Limited	England and Wales
General Motors Financial Chile Limitada	Chile
General Motors Financial Chile S.A.	Chile
General Motors Financial Company, Inc.	Texas
General Motors Financial International B.V.	Netherlands
General Motors Financial Italia S.p.A.	Italy
General Motors Financial of Canada, Ltd.	Ontario
General Motors Financial Suisse SA	Switzerland
General Motors Financial UK Limited	England and Wales
General Motors Finland Oy	Finland
General Motors Foundation, Inc.	Michigan
General Motors France	France
General Motors GBS Hungary Kft.	Hungary
General Motors Global Service Operations, Inc.	Delaware
General Motors Hellas S.A.	Greece
General Motors Holden Australia Ltd.	Australia
General Motors Holden Australia NSC Ltd.	Australia
General Motors Holdings LLC	Delaware
General Motors Holdings Participacoes Ltda.	Brazil
General Motors India Private Limited	India
General Motors International Holdings, Inc.	Delaware
General Motors International Operations Pte. Ltd.	Singapore
General Motors International Services Company SAS	Colombia
General Motors International Services LLC	Delaware
General Motors Investment Management Corporation	Delaware
General Motors Investment Participacoes Ltda.	Brazil
General Motors Investments Pty. Ltd.	Australia
General Motors Ireland Limited	Ireland
General Motors Israel Ltd.	Israel
General Motors IT Services (Ireland) Limited	Ireland
General Motors Italia S.r.l.	Italy
General Motors Japan Limited	Japan
General Motors Limited	England
General Motors LLC	Delaware
General Motors Manufacturing Poland Sp. z o.o.	Poland
General Motors Nederland B.V.	Netherlands

Company Name	State or Sovereign Power of Incorporation
General Motors New Zealand Pensions Limited	New Zealand
General Motors of Canada Company	Canada
General Motors Overseas Commercial Vehicle Corporation	Delaware
General Motors Overseas Corporation	Delaware
General Motors Overseas Corporation (active)	Delaware
General Motors Overseas Distribution LLC	Delaware
GENERAL MOTORS PARTICIPACOES LTDA.	Brazil
General Motors Peru S.A.	Peru
General Motors Poland Spolka, z o. o.	Poland
General Motors Portugal Lda.	Portugal
General Motors Powertrain - Europe S.r.l.	Italy
General Motors Powertrain - Uzbekistan CJSC	Uzbekistan
General Motors Powertrain - Uzbekistan Joint Stock Company	Uzbekistan
General Motors Powertrain (Thailand) Limited	Thailand
General Motors Research Corporation	Delaware
General Motors South Africa (Pty) Limited	South Africa
General Motors Suisse S.A.	Switzerland
General Motors Taiwan Ltd.	Taiwan
General Motors Technical Centre India Private Limited	India
General Motors Thailand Investments, LLC	Delaware
General Motors Treasury Center, LLC	Delaware
General Motors Trkiye Limited Sirketi	Turkey
General Motors UK Limited	England
General Motors Uruguay S.A.	Uruguay
General Motors Uzbekistan Closed Joint Stock Company	Uzbekistan
General Motors Venezolana, C.A.	Venezuela
General Motors Ventures LLC	Delaware
General Motors Vietnam Company Ltd.	Vietnam
General Motors Warehousing and Trading (Shanghai) Co. Ltd.	China
General Motors-Holden's Sales Pty. Limited	Australia
Genie Mecanique Zairois, S.A.R.L.	Congo, The Democratic Republic
GeoDigital International Inc.	Ontario
Georgia Automotive Group, Inc.	Delaware
Global Human Body Models Consortium, LLC	Michigan
Global Services Detroit LLC	Delaware
Global Tooling Service Company Europe Limited	England and Wales
Glympse Inc.	Washington
GM - Isuzu Camiones Andinos de Chile SpA	Chile
GM - Isuzu Camiones Andinos de Colombia Ltda.	Colombia
GM - Isuzu Camiones Andinos de Colombia S.A.	Colombia
GM - ISUZU Camiones Andinos del Ecuador GMICA Ecuador Cia. Ltda.	Ecuador

Company Name	State or Sovereign Power of Incorporation
GM (UK) Pension Trustees Limited	England
GM Administradora de Bens Ltda.	Brazil
GM APO Holdings, LLC	Delaware
GM Auslandsprojekte GmbH	Germany
GM Automotive Services Belgium NV	Belgium
GM Automotive UK	England
GM Canada Holdings B.V.	Netherlands
GM Canada Holdings LLC	Delaware
GM Canada Limited Partnership	Canada
GM CME Holdings C.V.	Netherlands
GM Components Holdings, LLC	Delaware
GM Cruise LLC	Delaware
GM Daewoo UK Limited	England
GM Deutschland GmbH	Germany
GM Eurometals, Inc.	Delaware
GM Europe Treasury Company AB	Sweden
GM Finance Co. Holdings LLC	Delaware
GM Financial AB	Sweden
GM Financial Automobile Leasing Trust 2014-1	Delaware
GM Financial Automobile Leasing Trust 2014-2	Delaware
GM Financial Automobile Leasing Trust 2014-PP1	Delaware
GM Financial Automobile Leasing Trust 2015-1	Delaware
GM Financial Automobile Leasing Trust 2015-2	Delaware
GM Financial Automobile Leasing Trust 2015-3	Delaware
GM Financial Automobile Leasing Trust 2015-PP1	Delaware
GM Financial Automobile Leasing Trust 2015-PP2	Delaware
GM Financial Automobile Leasing Trust 2015-PP3	Delaware
GM Financial Automobile Leasing Trust 2015-PP4	Delaware
GM Financial Automobile Leasing Trust 2015-PP5	Delaware
GM Financial Automobile Leasing Trust 2016-1	Delaware
GM Financial Automobile Leasing Trust 2016-2	Delaware
GM Financial Automobile Leasing Trust 2016-3	Delaware
GM Financial Automobile Leasing Trust 2016-PP1	Delaware
GM Financial Automobile Leasing Trust 2016-PP2	Delaware
GM Financial Automobile Leasing Trust 2016-PP3	Delaware
GM Financial Automobile Leasing Trust 2016-PP4	Delaware
GM Financial Automobile Leasing Trust 2016-PP5	Delaware
GM Financial Automobile Leasing Trust 2016-PP6	Delaware
GM Financial Automobile Leasing Trust 2016-PP7	Delaware
GM Financial Automobile Leasing Trust 2017-1	Delaware
GM Financial Automobile Leasing Trust 2017-2	Delaware

Company Name	State or Sovereign Power of Incorporation
GM Financial Automobile Leasing Trust 2017-PP1	Delaware
GM Financial Automobile Leasing Trust 2017-PP2	Delaware
GM Financial Automobile Leasing Trust 2017-PP3	Delaware
GM Financial Automobile Leasing Trust 2017-PP4	Delaware
GM Financial Automobile Receivables Trust 2012-PP1	Delaware
GM Financial Automobile Receivables Trust 2014-PP1	Delaware
GM Financial Canada Leasing Ltd.	Ontario
GM Financial Colombia Holdings LLC	Delaware
GM Financial Colombia S.A. Compania de Financiamiento	Colombia
GM Financial Consumer Automobile Receivables Trust 2017-1	Delaware
GM Financial Consumer Automobile Receivables Trust 2017-2	Delaware
GM Financial Consumer Automobile Receivables Trust 2017-3	Delaware
GM Financial Consumer Discount Company	Pennsylvania
GM Financial de Mexico, S.A. de C.V. SOFOM E.R.	Mexico
GM Financial de Mexico, S.A. de C.V., SOFOME.N.R.	Mexico
GM Financial del Peru S.A.C	Peru
GM Financial GmbH	Germany
GM Financial Holdings LLC	
GM Financial Insurance Services GmbH	Germany
GM Financial Management Trust	Delaware
GM Financial Mexico Holdings LLC	Delaware
GM Financial Real Estate GmbH & Co KG	Germany
GM GEFS HOLDINGS (CHC4) ULC	Nova Scotia
GM Global Business Services Philippines, Inc.	Philippines
GM Global Holdings GmbH & Co. KG	Germany
GM Global Propulsion Systems -Torino S.r.l.	Italy
GM Global Purchasing and Supply Chain Romania Srl	Romania
GM Global Technology Operations LLC	Delaware
GM Global Tooling Company LLC	Delaware
GM Global Treasury Centre Limited	England and Wales
GM Holden Ltd.	Australia
GM Holdings U.K. No.1 Limited	England and Wales
GM Holdings U.K. No.3 Limited	England and Wales
GM International Sales Ltd.	Cayman Islands
GM Inversiones Santiago Limitada	Chile
GM Investment Trustees Limited	England
GM Korea Co., Ltd	Korea, Republic of
GM Korea Company	Korea, Republic of
GM Korea Ltd.	Korea, Republic of
GM LAAM Holdings, LLC	Delaware
GM Mexico Holdings B.V.	Netherlands

Company Name	State or Sovereign Power of Incorporation
GM Nigeria Limited	Nigeria
GM Personnel Services, Inc.	Delaware
GM Plats (Proprietary) Limited	South Africa
GM PSA Purchasing Services S.A.	Belgium
GM Purchasing Vauxhall UK Limited	England
GM Regional Holdings LLC	Delaware
GM Retirees Pension Trustees Limited	England
GM Subsystems Manufacturing, LLC	Delaware
GM Supplier Receivables LLC	Delaware
GM Viet Nam Motor Company Ltd.	Vietnam
GM Warranty LLC	Delaware
GMAC - Instituicao Financeira de Credito, S.A.	Portugal
GMAC (Espana?) de Financiacion, S.A. Unipersonal	Spain
GMAC (Lease?) B.V. (aka Masterlease Europe)	Netherlands
GMAC Administradora de Consorcios Ltda.	Brazil
GMAC Automotriz Limitada	Chile
GMAC Bank GmbH (German entity)	Germany
GMAC Banque S.A.	France
GMAC Colombia S.A. LLC	Delaware
GMAC Comercial Automotriz Chile S.A.	Chile
GMAC Continental Corporation	Delaware
GMAC de Venezuela, C.A.	Venezuela
GMAC Espana de Financiacion, S.A. Unipersonal	Spain
GMAC Financial Services AB	Sweden
GMAC Financial Services GmbH	Germany
GMAC HB	Sweden
GMAC Holding S.A. de C.V.	Mexico
GMAC Holdings (U.K.) Limited	England
GMAC Holdings UK Limited	England
GMAC Lease B.V. (aka Masterlease Europe)	Netherlands
GMAC Leasing GmbH (Austrian entity)	Austria
GMAC Leasing GmbH (German entity)	Germany
GMAC Nederland N.V.	Netherlands
GMAC Prestadora de Servicios de Mao de Obra Ltda.	Brazil
GMAC Real Estate GmbH & Co KG	Germany
GMAC Servicios S.A.S.	Colombia
GMAC Suisse SA	Switzerland
GMAC UK plc	England
GMACI Corretora de Seguros Ltda	Brazil
GMACI Corretora de Seguros S.A.	Brazil
GMAC-Prestadora de Servios de Mo-de-Obra Ltda.	Brazil

Company Name	State or Sovereign Power of Incorporation
GMAM Real Estate I, LLC	Delaware
GM-AVTOVAZ CJSC	Russian Federation
GMCH&SP Private Equity II L.P.	Canada
GM-DI Leasing LLC	Delaware
GMF Automobile Leasing Trust 2013-(PP1?)	Delaware
GMF Europe Holdco Limited	United Kingdom
GMF Europe LLP	England and Wales
GMF Floorplan Owner Revolving Trust	Delaware
GMF Funding Corp.	Delaware
GMF Germany Holdings GmbH	Germany
GMF Global Assignment LLC	Delaware
GMF International LLC	Delaware
GMF Leasing LLC	Delaware
GMF Leasing Warehouse Trust 2016-A	Delaware
GMF Leasing Warehouse Trust 2016-B	Delaware
GMF Leasing Warehousing Trust	Delaware
GMF Prime Automobile Trust 2015-PP1	Delaware
GMF Prime Automobile Trust 2016-PP1	Delaware
GMF Prime Automobile Trust 2016-PP2	Delaware
GMF Prime Automobile Trust 2016-PP3	Delaware
GMF Prime Automobile Trust 2017-PP1	Delaware
GMF Prime Automobile Trust 2017-PP2	Delaware
GMF Prime Automobile Trust 2017-PP3	Delaware
GMF Prime Automobile Trust 2017-PP4	Delaware
GMF Prime Automobile Warehouse Trust I	Delaware
GMF Prime Automobile Warehouse Trust II	Delaware
GMF Prime Automobile Warehouse Trust III	Delaware
GMF Prime Automobile Warehouse Trust IV	Delaware
GMF Prime Automobile Warehouse Trust IX	Delaware
GMF Prime Automobile Warehouse Trust V	Delaware
GMF Prime Automobile Warehouse Trust VI	Delaware
GMF Prime Automobile Warehouse Trust VII	Delaware
GMF Prime Automobile Warehouse Trust VIII	Delaware
GMF Prime Automobile Warehouse Trust X	Delaware
GMF Prime Automobile Warehouse Trust XI	Delaware
GMF Prime Automobile Warehouse Trust XII	Delaware
GMF Prime Automobile Warehouse Trust XIII	Delaware
GMF Prime Automobile Warehouse Trust XIV	Delaware
GMF Wholesale Receivables LLC	Delaware
GMGP Holdings LLC	Delaware
GM-UM1 Technology Research and Development Ltd.	Israel

Company Name	State or Sovereign Power of Incorporation
Go Motor Retailing Limited	England and Wales
Go Trade Parts Limited	England and Wales
Gochip Inc.	California
GP Global Holdings GmbH	Germany
GPSC UK Limited	England and Wales
Grand Pointe Holdings, Inc.	Michigan
Grand Pointe Park Condominium Association	Michigan
H.S.H. Limited	England and Wales
Haines & Strange Limited	England and Wales
Heritage Chevrolet Cadillac Buick GMC, Inc.	Delaware
HOLDCORP S.A.	Ecuador
Holden Employees Superannuation Fund Pty Ltd	Australia
Holden New Zealand Limited	New Zealand
HRL Laboratories, LLC	Delaware
Hydrogenics Corporation	Ontario
IBC 2017 Pension Trustees Limited	United Kingdom
IBC Pension Trustees Limited	England
IBC Vehicles Limited	England
Industries Mecaniques Maghrebines, S.A.	Tunisia
Infinite Velocity Automotive, Inc.	Delaware
ISF International School Frankfurt Rhein-Main GmbH & Co. KG	Germany
ISF Internationale Schule Frankfurt-Rhein-Main Geschaftsfuhrungsgesellschaft mbH	Germany
Isuzu Truck South Africa (Pty.) Limited (ITSA)	South Africa
IUE-GM National Joint Skill Development and Training Committee	Ohio
Jeffery (Wandsworth) Limited	England and Wales
JS Folsom Automotive, Inc.	Delaware
Kalfatra Utveckling AB	Sweden
Kamp Twente B.V.	Netherlands
Koneyren, Inc.	Michigan
Lakeside Chevrolet Buick GMC Ltd.	Ontario
Laplante Cadillac Chevrolet Buick GMC Ltd.	Ontario
LCV Platform Engineering Corp.	Japan
Lease Ownership Cooperative LLC	Delaware
Lidlington Engineering Company, Ltd.	Delaware
Limited Liability Company "General Motors CIS"	Russian Federation
Limited Liability Company "JV Systems"	Russian Federation
Lookers Birmingham Limited	England and Wales
Lufkin Automotive Group, Inc.	Delaware
Lyft, Inc.	Delaware
MAC International FZCO	United Arab Emirates
Mack Buick-GMC, Inc.	Delaware

Company Name	State or Sovereign Power of Incorporation
Mack-Buick-GMC, Inc.	Delaware
Macon County Automotive Group, Inc.	Delaware
Manassas Chevrolet, Inc.	Delaware
Marshall of Ipswich Limited	England and Wales
Marshall of Peterborough Limited	England and Wales
Marshall of Stevenage Ltd	England and Wales
Martin Automotive of Simi Valley, Inc.	Delaware
Martin Automotive, Inc.	Delaware
Mascoma Corporation	Delaware
Master Lease Germany GmbH	Germany
Masterlease Europe Renting, S.L.	Spain
Maven Drive LLC	Delaware
Maven Leasing Ltd.	Delaware
Memorial Highway Chevrolet, Inc.	Delaware
Merced Chevrolet, Inc.	Delaware
Michael Bates Chevrolet, Inc.	Delaware
Mike Reichenbach Chevrolet, Inc.	Delaware
Millbrook Pension Management Limited	England
Missouri Automotive Group, Inc.	Delaware
Monetization of Carve-Out, LLC	Delaware
Monetization of Carve-Out, LLC	Delaware
Motor Repris Automocio S.L.	Spain
Motorbodies Luton Limited	England and Wales
Motors Holding LLC	Delaware
Motors Properties (Trading) Limited	England and Wales
Motors Properties Limited	England and Wales
Multi-Use Lease Entity Trust	Delaware
Murketts of Cambridge Limited	England and Wales
Nauto, Inc.	Delaware
Neovia Logistics Supply Chain Services GmbH	Germany
NJDOI/GMAM Core Plus Real Estate Investment Program, L.P.	Delaware
NJDOI/GMAM Opportunistic Real Estate Investment Program, L.P.	Delaware
NJDOUGMAM Core Plus Real Estate Investment Program, L.P.	Delaware
North American New Cars LLC	Delaware
North American New Cars, Inc.	Delaware
Novasentis, Inc.	Delaware
Now Motor Retailing Limited	England and Wales
OEC Midco, LLC	Delaware
OEConnection Holdings,LLC	Delaware
OEConnection LLC	Delaware
OEConnection Manager Corp.	Delaware

Company Name	State or Sovereign Power of Incorporation
Omnibus BB Transportes, S. A.	Ecuador
OnStar Connected Services Srl	Romania
OnStar de Mexico S. de R.L. de C.V.	Mexico
OnStar Europe Ltd.	England and Wales
OnStar Global Services Corporation	Delaware
OnStar Middle East FZ-LLC	United Arab Emirates
OnStar, LLC	Delaware
Opel Australia Pty Ltd	Australia
Opel Automobile GmbH	Germany
Opel Bank GmbH	Germany
Opel Danmark A/S	Denmark
Opel Finance B.V.B.A.	Belgium
Opel Group GmbH	Germany
Opel Group Warehousing GmbH	Germany
Opel Leasing GmbH (German entity)	Germany
Opel Norge AS	Norway
Opel Sonderdienste GmbH	Germany
Opel Southeast Europe LLC	Hungary
Opel Special Vehicles GmbH	Germany
Opel Suisse SA	Switzerland
Opel Sverige AB	Sweden
Opel Szentgotthard Automotive Manufacturing LLC	Hungary
Opel Szentgotthard Automotive Manufacturing Ltd	Hungary
Opel Wien GmbH	Austria
Open Synergy GmbH	Germany
Orange Motors B.V.	Netherlands
OT Mobility, Inc.	Delaware
P. T. Mesin Isuzu Indonesia	Indonesia
P.T. G M AutoWorld Indonesia	Indonesia
P.T. General Motors Indonesia	Indonesia
Pan Asia Technical Automotive Center Company, Ltd.	China
Patriot Chevrolet, Inc.	Delaware
Pearl (Crawley) Limited	England and Wales
Performance Equity Management, LLC	Delaware
Peter Vardy (Perth) Limited	Scotland
PIMS Co.	Delaware
Plan Automotor Ecuatoriano S.A. Planautomotor	Ecuador
Powermat Technologies Ltd.	Israel
Princeton Chevrolet, Inc.	Delaware
Private Auto Lease Trust	Delaware
Promark Global Advisors Limited	England

Company Name	State or Sovereign Power of Incorporation
ProSTEP AG	Germany
Proterra Inc	Delaware
PT. General Motors Indonesia Manufacturing	Indonesia
Quality Chevrolet, Inc.	Delaware
Quantum Fuel Systems Technologies Worldwide, Inc.	Delaware
Randstad WorkNet GmbH	Germany
Reeve (Derby) Limited	England and Wales
Reeve (Lincoln) Ltd	England and Wales
Reeve (Sheffield) Limited	England and Wales
Reg Vardy (VMC) Limited	England and Wales
RelayRides, Inc.	Delaware
Renton Cadillac Pontiac GMC, Inc.	Delaware
Riverfront Holdings III, Inc.	Delaware
Riverfront holdings Phase II, Inc.	Delaware
Riverfront Holdings, Inc.	Delaware
RMH III, Inc.	Delaware
Ruedas de Aluminio, C.A.	Venezuela
S.C. UNION MOTORS CAR SALES S.L.R.	Romania
Saab Automobile AB	Sweden
Saab Finance Limited	England
Saankhya Labs Pvt. Ltd.	India
SAIC General Motors Corporation Limited	China
SAIC General Motors Investment Limited	China
SAIC General Motors Investment Limited	Hong Kong
SAIC General Motors Sales Company Limited	China
SAIC GM (Shenyang) Norsom Motors Co., Ltd.	China
SAIC GM Dong Yue Motors Company Limited	China
SAIC GM Dong Yue Powertrain Company Limited	China
SAIC GM Wuling Automobile Company Limited	China
SAIC Motor Insurance Sales Company Limited	China
SAIC-GMAC Automotive Finance Company Limited	China
Sakti3, Inc.	Delaware
Salmon Street Ltd.	Australia
Sandoval Buick GMC, Inc.	Delaware
Sarmiento 1113 S.A. (en liquidacion)	Argentina
Savari Inc.	California
SB (Helston) Limited	England and Wales
Scranton Chevrolet of Norwich, Inc.	Delaware
SDC Materials, Inc.	Delaware
Servicios GMAC S.A. de C.V.	Mexico
Seward (Wessex) Limited	England and Wales

Company Name	State or Sovereign Power of Incorporation
Shanghai Chengxin Used Car Operation and Management Company Limited	China
Shanghai General Motors Corporation Ltd.	China
Shanghai GM (Shenyang) Norsom Motors Co. Ltd..	China
Shanghai GM Dong Yue Motors Company Limited	China
Shanghai GM Dong Yue Powertrain Company Limited	China
Shanghai OnStar Telematics Co. Ltd.	China
Sherwoods (Darlington) Limited	England and Wales
Simpson Garden Grove, Inc.	Delaware
Simpson Irvine, Inc.	Delaware
Sirrus, Inc.	Delaware
Sistemas de Compra Programada Chevrolet, C.A.	Venezuela
Skurrays Limited	England
Skurrays Motors Limited	England and Wales
Slaters (GM) Limited	England and Wales
Smokey Point Buick Pontiac GMC, Inc.	Delaware
SolidEnergy Systems Corp.	Delaware
South Haven Chevrolet Buick GMC, Inc.	Delaware
Southern (Merthyr) Limited	England and Wales
State Line Buick GMC, Inc.	Delaware
Sterling Motor Properties Limited	England and Wales
Strobe, Inc.	Delaware
Superior Chevrolet, Inc.	Delaware
Tactus Technology, Inc.	Canada
Temis Chevrolet Buick GMC Ltee	Delaware
The NanoSteel Company, Inc.	England and Wales
Thurlow Nunn (JV) Limited	England and Wales
Thurlow Nunn (MV) Limited	Delaware
TJP Enterprises, Inc.	Delaware
Todd Wenzel Buick GMC of Davison, Inc.	Delaware
Todd Wenzel Buick GMC of Westland, Inc.	Delaware
Tradition Chevrolet Buick, Inc.	Delaware
Tula Technology, Inc.	England and Wales
Tustain Motors Limited	Germany
TÜV NORD Bildung Opel GmbH	Romania
Union Motors Car Sales S.r.l.	Michigan
United States Advanced Battery Consortium, LLC	Michigan
United States Automotive Materials Partnership, LLC	Michigan
United States Council for Automotive Research LLC	Delaware
Valentine Buick GMC, Inc.	Netherlands
Van Kouwen Automotive I B V	England and Wales
Vauxhall Defined Contribution Pension Plan Trustees Limited	

Company Name	State or Sovereign Power of Incorporation
Vauxhall Motors Limited	England
Vehicle Asset Universal Leasing Trust	Delaware
Velocity Prime Automotive, Inc.	Delaware
Vence Lone Star Motors, Inc.	Delaware
Vertu Motors (Chingford) Limited	England and Wales
Vertu Motors (VMC) Limited	England and Wales
VHC Sub-Holdings (UK)	England
Vickers (Lakeside) Limited	England and Wales
Vision Motors Limited	England and Wales
VML 2017 Pension Trustees Limited	United Kingdom
VMO Properties Limited	England and Wales
VRP Venture Capital Rheinland-Pfalz Nr. 2 GmbH & Co. KG	Germany
Waterpaper Limited	England and Wales
Welcome S.R.L.	Italy
Wheatcroft (Worksop) Limited	England and Wales
Whitehead (Rochdale) Limited	England and Wales
William Grimshaw & Sons Limited	England
Wilson & Co. (Motor Sales) Limited	England and Wales
Wind Point Partners III, L.P.	Delaware
Woodbridge Buick GMC, Inc.	Delaware
WRE, Inc.	Michigan
Yi Wei Xing (Beijing) Technology Co., Ltd.	China
Zona Franca Industrial Colmotores SAS	Colombia

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT 17 APR 21 A 11: 18

In Re: GORDON WATSON	)	CIVIL DIVISION
	)	Docket No. 259-4-17 Wncv

ASSURANCE OF DISCONTINUANCE

The State of Vermont, by and through Vermont Attorney General Thomas J. Donovan, Jr., and Gordon Watson ("Respondent"), hereby enter into this Assurance of Discontinuance ("AOD") pursuant to 9 V.S.A. § 2459.

Regulatory Framework

1. Lead-based paint in housing, the focus of the Vermont lead law, is a leading cause of childhood lead poisoning, which can result in adverse health effects, including decreases in IQ.
2. All paint in pre-1978 housing is presumed to be lead-based unless a certified inspector has determined that it is not lead-based. 18 V.S.A. § 1759(a).
3. All paint in rental target housing is "presumed to be lead-based unless a lead inspector or lead risk assessor has determined that it is not lead-based." 18 V.S.A. § 1760(a).
4. The lead law requires that essential maintenance practices ("EMPs") specified in 18 V.S.A. § 1759 be performed at all pre-1978 rental housing.
5. EMPs include, but are not limited to, installing window well inserts, visually inspecting properties at least annually for deteriorated paint, restoring surfaces to be free of deteriorated paint within 30 days after such paint has been visually identified

Office of the ATTORNEY GENERAL
109 State Street
Montpelier, VT 05609

or reported to the owner, and posting lead-based paint hazard information in a prominent place. 18 V.S.A. § 1759(a) (2), (4) and (7).

6. The EMP requirements also mandate that an owner of rental target housing file affidavits or compliance statements attesting to EMP performance with the Vermont Department of Health and with the owner's insurance carrier. 18 V.S.A. § 1759(b).
7. A violation of the lead law requirements may result in a maximum civil penalty of $10,000.00. 18 V.S.A. § 130(b)(6). Each day that a violation continues is a separate violation. 18 V.S.A. § 130(b)(6).
8. The Vermont Consumer Protection Act, 9 V.S.A Chapter 63, prohibits unfair and deceptive acts and practices, which includes the offering for rent, or the renting of, target housing that is noncompliant with the lead law.
9. Violations of the Consumer Protection Act are subject to a civil penalty of up to $10,000.00 per violation. 9 V.S.A. § 2458(b)(1). Each day that a violation continues is a separate violation.

Respondent's Rental Housing and Lead Compliance Practices

10. Respondent is the owner of four rental properties located at: 176 Main Street North, Bakersfield; 15 Third Street, Barre City; 56 Long Street, Barre City; and 16 Mt. Vernon Place, Barre City (collectively, "the Properties").
11. The Properties were all constructed prior to 1978, and therefore, are pre-1978 "rental target housing" within the meaning of the Vermont lead law, 18 V.S.A. § 1751(23), and are all subject to the requirements of 18 V.S.A. Chapter 38.
12. Respondent has in the past and continues presently to rent and offer for rent units in the Properties.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

13. On August 11, 2016, the Vermont Department of Health sent a "Notice of Non-Compliance" indicating that Respondent had not filed an "EMP Rental Property Compliance Statement" for the property at 176 Main Street North. The Department allowed for 30 days for Respondent to file the necessary statements.

14. Respondent did not respond to the 30-day Notice, and did not file EMP compliance statements within 30 days.

15. As of March 2017, Respondent has not filed current EMP compliance statements for all four rental properties.

16. Respondent admits the truth of the facts described in ¶¶ 10-15.

The State's Allegations

17. The Vermont Attorney General's Office alleges the following violations of the Consumer Protection Act and Lead Law:

    a. Failing to file EMP compliance statements for rental properties.

18. The State of Vermont alleges that the above behavior constitutes unfair and deceptive acts and practices under 9 V.S.A. § 2453.

Assurances and Relief

In lieu of instituting an action or proceeding against Respondent, the Attorney General and Respondent are willing to accept this AOD pursuant to 9 V.S.A. § 2459. Accordingly, the parties agree as follows:

19. Respondent shall fully and timely comply with the requirements of the Vermont lead law, 18 V.S.A., Chapter 38, as long as they maintain any ownership or property management interest in the Properties and in any other pre-1978 rental housing in

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

which they currently have, or later acquire, an ownership or property management interest.

20. By April 25, 2017, Respondent shall complete all EMP inspections and work of the Properties (as specified in 18 V.S.A. § 1759), giving priority to the Properties where a child age 6 or under is residing. Pursuant to 18 V.S.A. § 1759(a)(3), exterior work of the properties may be postponed until May 31, 2017, so long as access to exterior surfaces and components of the Properties with lead hazards and areas directly below the deteriorated surfaces are clearly restricted. All interior work must be completed by the April 25, 2017 deadline. If Respondent requires additional time to complete the work, Respondent will contact the Attorney General's Office before the expiration of the above deadlines and provide a detailed justification for any extension.

21. Within one week of completion of the EMP work at the Properties described in the paragraph above, Respondent will file with the Vermont Department of Health, Respondent's insurance carrier and with the Office of the Attorney General, a completed EMP compliance statement for all Properties, and will give a copy of the compliance statement to an adult in each rented unit of all Properties. The copy for the Office of the Attorney General shall be sent to: *Justin Kolber, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.*

22. In the event Respondent wishes to rent a unit which becomes vacant in any of Respondent's pre-1978 rental housing before such housing is made EMP compliant, Respondent shall provide advance written notice of the intent to rent to the Office of

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

the Attorney General at the address listed above. Respondent's advance written notice shall also: (1) verify that the interior of the specific unit to be rented is EMP compliant; (2) provide an update as to any remaining EMP work to be performed at the property, including the date by which the entire property will be EMP compliant. Otherwise, Respondent shall not rent, or offer for rent, any unit which becomes vacant in any of property owned or managed by Respondent that is not EMP compliant until such time as the EMP work is complete and the EMP compliance statement is distributed as described above.

23. Respondent shall pay the sum of $3,500 in civil penalties and costs for the failure to file EMP compliance statements, with $1,500 being paid no later than May 31, 2017, and the remaining $2,000 to be paid no later than August 31, 2017. All payments shall be a single check payable to "the State of Vermont" and sent to the Office of the Attorney General at the address listed in paragraph 21.

24. Respondent shall pay the costs of any follow-up compliance inspections as determined by the Attorney General's Office.

Other Terms

25. This AOD is binding on Respondent, however, sale of any pre-1978 rental property may not occur unless Respondent has complied with all obligations under this AOD, or this AOD is amended in writing to transfer to the buyer or other transferee all remaining obligations.

26. Transfer of ownership of any of Respondent's pre-1978 rental properties shall be consistent with Vermont law, including the provisions of 18 V.S.A. § 1767 specifically relating to the transfer of ownership of pre-1978 rental housing.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

27. This AOD shall not affect marketability of title.

28. Nothing in this AOD in any way affects Respondent's other obligations under state, local, or federal law.

29. In addition to any other penalties or relief which might be appropriate under Vermont law, any future failure by Respondent to comply with the terms of this AOD shall be subject to a liquidated civil penalty paid to the State of Vermont in the amount of at least $5,000 and not more than $10,000.

SIGNATURES APPEAR ON NEXT PAGE

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

DATED at Montpelier, Vermont this 7th day of April, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____
Justin E. Kolber
Assistant Attorney General
Office of the Attorney General
109 State Street
Montpelier, VT 05609
(802) 828-5620
justin.kolber@vermont.gov

DATED at ESSEX, Vermont this 17 day of April, 2017.

GORDON WATSON

By: _____
Gordon Watson

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

IN RE: GRAND BUFFET ESSEX JUNCTION INC., TOM LI, and ZHIHUA "JOYCE" LI	)	CIVIL DIVISION Docket No. 106-2-17 Wncv

ASSURANCE OF DISCONTINUANCE

Vermont Attorney General Thomas J. Donavan, Jr. ("the Attorney General") and Grand Buffet Essex Junction Inc., Tom Li, and Zhihua "Joyce" Li ("Respondents") hereby agree to this Assurance of Discontinuance ("AOD") pursuant to 9 V.S.A. § 2459.

BACKGROUND

1. Respondent Grand Buffet Essex Junction Inc. ("Grand Buffet") is a domestic profit corporation incorporated under the laws of Vermont, with its principal place of business located at 66 Pearl Street, Essex Junction, Vermont. Grand Buffet is a restaurant serving Chinese-style cuisine.

2. Respondent Tom Li is a resident of Essex Junction, Vermont. Tom Li is the president and director of Grand Buffet.

3. Respondent Zhihua "Joyce" Li is a resident of Essex Junction, Vermont. Joyce Li is the manager of Grand Buffet.

4. In late 2012, a Grand Buffet employee stole customers' credit card information and credit card fraud was committed. The matter was referred to law enforcement and the Attorney General made recommendations to Respondents for operational changes that would prevent a repetition of the incident.

5. Grand Buffet did not consistently implement the recommendations.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

6. In July 2014, at least 79 customers had their credit card numbers stolen from Grand Buffet, resulting in over $20,000 worth of credit card fraud.

7. In December 2014, at least 20 customers had their credit card numbers stolen from Grand Buffet, resulting in over $15,800 worth of credit card fraud.

8. These numbers only indicate the amount of fraud identified; the actual number of credit cards stolen and the actual amount of fraud may likely be higher.

9. Respondents have not complied with their record-keeping obligations under state and federal law regarding the employees that they hired.

10. Respondents had a heightened obligation to prevent fraud from taking place at their business, after they became aware of the fraud that took place in late 2012 and received the Attorney General's recommendations.

11. Respondents have failed to take sufficient reasonable measures to prevent credit card information from being stolen at Grand Buffet.

12. Failure to take reasonable measures to protect the security of consumers' credit card information constitutes an unfair act and practice under 9 V.S.A. § 2453.

13. In February 2017, the three individuals who committed the credit card fraud, one ex-employee of Grand Buffet who stole the credit card numbers, and two accomplices who used the counterfeit credit cards; were sentenced and ordered to jointly pay $25,608.33 restitution to the victim banks and credit unions that suffered the losses due to the fraud.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

INJUNCTIVE RELIEF

Changes in Operating Systems

14. Starting immediately, Respondents shall implement the following operational safeguards:

a. Maintain appropriate oversight of their employees and how they handle customer credit cards;

b. Either only collect customers' credit card information at the hostess stand, and do not permit wait-staff to handle customers' credit cards, or implement technology to swipe credit cards at the table; and

c. Require use of an identification code unique to each employee authorized to handle credit cards to be used when submitting customers' credit card information.

Record Keeping

15. Starting immediately, Grand Buffet shall comply with all record-keeping requirements regarding its employees, including:

a. Timely completion and submission of Department of Labor Form C-101 on a quarterly basis, listing gross wages paid to all employees in the previous calendar quarter;

b. Reporting all newly-hired employees to the Department of Labor within ten days of hire, either by paper Form C-61 or online at: https://uipublic.labor.vermont.gov/EmployerPortal/EmployerFunctions/apphome.aspx. Grand Buffet shall keep a copy of each such report for at least three years.

Office of the
ATTORNEY
GENERAL
109 State Street
Montpelier, VT
05609

c. Providing each employee with a weekly, bi-weekly or semi-monthly paycheck statement listing in detail gross wages earned, net wages paid, and all deductions made for state and federal taxes and other required or authorized deductions. Grand Buffet shall keep a copy of each such statement for at least three years.

d. Completing a USDOL Employment Eligibility Verification Form (I-9) for each employee. Grand Buffet shall keep a copy of that form for at least three years.

16. Respondents shall comply with all provisions of Vermont's Consumer Protection Act, 9 V.S.A. §§ 2451-2480.

PENALTIES

17. Respondents agree to a civil penalty of Thirty Thousand Dollars ($30,000.00) of which Respondents must pay Two-Thousand, Five-Hundred Dollars ($2,500.00) within ten days of both Parties signing this AOD (the "Effective Date"), and Two-Thousand, Five-Hundred Dollars ($2,500.00) each month thereafter until the full amount is paid. The full amount must be paid within one year of the Effective Date. Respondents shall make payments to the "State of Vermont" and send payments to: Ryan Kriger, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

REPORTING

18. To determine or secure compliance with this Assurance of Discontinuance, on reasonable notice given to Respondents, subject to any lawful privilege:

a. Duly authorized representatives of the Attorney General, including representative of any other law enforcement agency acting at the request of the Attorney General, shall be permitted access during normal office hours to inspect and copy all books, ledgers, accounts, correspondence, memoranda and other documents and records in the possession, custody, or control of Respondents, which may have counsel present, and the documents and records to be inspected and copied relate to the violations described in this Assurance of Discontinuance.

b. Respondent shall submit written reports, under oath if requested by the Attorney General, with respect to any matters contained in this Assurance of Discontinuance.

OTHER TERMS

19. Respondents agree that this Assurance of Discontinuance shall be binding on Respondents, and their successors and assigns.

20. The Attorney General hereby releases and discharges any and all claims arising under the Consumer Protection Act, 9 V.S.A. §§ 2451-2480, that it may have against Respondents for the conduct described in the Background section prior to December 31, 2014.

21. The Superior Court of the State of Vermont, Washington Unit, shall have jurisdiction over this Assurance and the parties hereto for the purpose of enabling the Attorney General to apply to this Court at any time for orders and directions as may be necessary or

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

appropriate to enforce compliance with or to punish violations of this Assurance of Discontinuance.

22. Acceptance of this AOD by the Vermont Attorney General's Office shall not be deemed approval by the Attorney General of any practices or procedures of Respondent not required by this AOD, and Respondent shall make no representation to the contrary.

STIPULATED PENALTIES

23. If the Superior Court of the State of Vermont, Washington Unit enters an order finding Respondents to be in violation of this Assurance of Discontinuance, then the parties agree that penalties to be assessed by the Court for each act in violation of this Assurance of Discontinuance shall be Five Thousand Dollars ($5,000.00). A future data Security breach at Grand Buffet shall not, alone, be evidence that Respondents violated this Assurance of Discontinuance.

NOTICE

24. Respondents may be located at: 66 Pearl Street, Essex Junction, Vermont.

25. Respondents shall notify the Attorney General of any change of business name or address within 20 business days.

26. For a period of twenty (20) years from the Effective Date, in the event that Tom Li or Zhihua "Joyce" Li obtains any ownership or managerial interest in any other business in Vermont, Respondent(s) shall notify the Attorney General of the name and address of the business within 20 business days.

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

SIGNATURE

In lieu of instituting an action or proceeding against Respondents, the Office of the Attorney General, pursuant to 9 V.S.A. § 2459, accepts this Assurance of Discontinuance. By signing below, Respondent(s) voluntarily agree with and submit(s) to the terms of this Assurance of Discontinuance.

DATED at Essex Junction, Vermont, this 15th day of February, 2017.

Tom Li, on behalf of himself and
Grand Buffet Essex Junction, Inc.

Zhihua "Joyce" Li

ACCEPTED on behalf of the Attorney General:

DATED at Montpelier, Vermont this 15th day of February, 2017.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By:

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

Office of the ATTORNEY GENERAL 109 State Street Montpelier, VT 05609

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

IN RE: HILTON DOMESTIC OPERATING COMPANY INC.	)	CIVIL DIVISION
	)	Docket No. 623-10-17 Wnw
	)	
	)	

ASSURANCE OF DISCONTINUANCE

This Assurance of Discontinuance ("Assurance") is entered into between the State of Vermont ("State"), and Respondent Hilton Domestic Operating Company Inc., as successor in interest to Park Hotels & Resorts Inc. f/k/a Hilton Worldwide, Inc., including all of its subsidiaries, affiliates, successors, and assigns ("Hilton" or "Respondent," and, together with the State, the "Parties"). This Assurance applies only to Hilton owned or managed properties and does not apply to franchise properties, where Hilton does not maintain a majority interest.

This Assurance resolves the State of Vermont's concerns regarding Hilton's compliance with the Vermont Security Breach Notice Act, 9 V.S.A. §§ 2430-35 and Consumer Protection Act, 9 V.S.A. Chapter 63.

I. PARTIES

1. The State is acting through its Attorney General with its office located at 109 State Street, Montpelier, Vermont, 05609.

2. Respondent Hilton is one of the largest hospitality companies in the world, with a portfolio of 14 brands comprising more than 4,900 properties with more than 796,000 rooms in 104 countries and territories. The company's portfolio includes Hilton Hotels & Resorts, Waldorf Astoria Hotels & Resorts, Conrad Hotels & Resorts, DoubleTree by Hilton, Embassy Suites by Hilton, Hilton Garden Inn, Homewood Suites by Hilton, and

Hilton Grand Vacations. Its principal business address is 7930 Jones Branch Dr., McLean, Virginia 22102. The undersigned is fully authorized to execute this Assurance on behalf of Hilton. Hilton is the primary global operating company of the Hilton family of companies and it and its subsidiaries hold the operating assets, contracts, intellectual property, and employees.

II. BACKGROUND

3. Vermont's Security Breach Notice Act:

(a) Defines "security breach" to mean "unauthorized acquisition of electronic data *or a reasonable belief of an unauthorized acquisition of electronic data* that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information maintained by the data collector." 9 V.S.A. § 2430(8)(A);

(b) Requires a data collector that experiences a security breach that affects Vermont residents to notify the Attorney General within 14 business days of the data collector's discovery of the security breach ("14-Day Notice"). 9 V.S.A. § 2435(b)(3)(B)(i); and

(c) Requires notice to consumers to be made "in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency . . . or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system."

4. In 2014 and 2015, Hilton experienced two separate network intrusions involving collection of credit card information.

5. Hilton first became aware of the First Incident on February 10, 2015, when Hilton was notified by its managed security services provider of a security incident involving one of its servers.

6. Hilton engaged a PCI Forensic Investigator ("PFI") on February 14, 2015, to begin scoping conversations, and formally retained the PFI for the First Incident on February 27, 2015.

7. On March 10, 2015 (28 days post-notification of the First Incident), the PFI issued a Preliminary Incident Response Report regarding the First Incident. The PFI found evidence of malware on a Hilton server, including evidence of malware designed to target payment card information.

8. The PFI was unable to determine how the attacker gained access to Hilton's computer network, potentially due in part to the fact that in March 2015, computers that might have contained relevant evidence were rebuilt as part of regular maintenance. Also, certain log files that could have contained relevant evidence were not centrally aggregated.

9. The PFI did not find definitive evidence of exfiltration of payment card data.

10. In the Preliminary Incident Response Report, the PFI estimated that the investigation would conclude on June 1, 2015.

11. In light of the PFI Preliminary assessment, the absence of computers and logs that might be necessary to investigate the incident, and the need to move expediently and without unreasonable delay, the Attorney General alleges that Hilton's duty to notify consumers of the First Incident was triggered on March 10, 2015 at the latest.

12. The Attorney General alleges that at this point Hilton had sufficient information to trigger the duty to provide 14-Day Notice to the Attorney General.

13. During this period, the Attorney General was in regular contact with counsel for Hilton due to an unrelated breach of an independently-owned Hilton managed property. Any mention of the First Incident would have satisfied the 14-Day Notice requirement.

14. On July 13, 2015, Hilton internally identified a second security incident. This was the earliest date of notification or discovery of the Second Incident.

15. Hilton engaged the same PFI to begin scoping conversations on July 30, 2015 and formally retained the PFI for the Second Incident on August 7, 2015.

16. On August 16, 2015, the PFI issued a Preliminary Incident Response Report regarding the Second Incident. The PFI identified evidence of malware that was designed to target payment card information. The PFI did not identify evidence of the exfiltration of payment card information.

17. The Attorney General alleges that Hilton's duty to notify consumers of the Second Incident was triggered on August 16, 2015 at the latest.

18. On October 2, 2015, Hilton received a Common Point of Purchase notification from a credit card issuing bank.

19. On November 24, 2015, Hilton notified the Vermont Office of the Attorney General of both security breaches, and provided substitute notice to consumers. This was 287 days after the Attorney General alleges that Hilton was notified of the First incident and 100 days after Hilton was notified of the Second Incident.

20. Hilton did not provide notice to the Vermont Office of the Attorney General within fourteen days of the Second Incident.

21. The Attorney General alleges that Hilton did not provide notice to consumers in the most expedient time possible and without unreasonable delay.

22. On March 16, 2016, the PFI issued its Final Incident Report regarding the First Incident.

23. The Payment Card Industry Data Security Standard ("PCI DSS") is a proprietary information security standard for organizations that process branded credit cards from the major card companies, including Visa, MasterCard, American Express, Discover, and JCB. The standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council to ensure cardholder data is processed in a secure environment.

24. The PFI found that Hilton was not in compliance with certain PCI DSS requirements.

25. On September 23, 2016, the PFI issued its Final Incident Report regarding the Second Incident.

26. As described in its report on the second infiltration, the PFI found that Hilton was not in compliance with certain PCI DSS requirements.

27. Failure to maintain reasonable security standards is a violation of Vermont's Consumer Protection Act, 9 V.S.A. § 2453.

III. ENJOINED CONDUCT

Pursuant to 9 V.S.A. § 2458, Respondent is hereby enjoined as follows:

General Data Security and Notice Practices

28. Respondent shall maintain reasonable data security policies and procedures designed to protect cardholder data, as defined in PCI DSS Version 3.2, attached hereto as Exhibit A ("Cardholder Data").

29. Respondent shall provide notice to affected Vermont residents and the Attorney General of a "Security breach" (as defined by 9 V.S.A. § 2430(8)) involving PII of Consumers (as defined by 9 V.S.A § 2430(2)) in compliance with 9 V.S.A. § 2435. In determining whether there has been an "unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data" pursuant to 9 V.S.A. § 2430(8), Respondent shall consider all information reasonably available to it, including, among other things, (i) indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information; (ii) indications that the information has been downloaded or copied; (iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; (iv) that the information has been made public; and (v) evidence of malware on its computer systems designed to collect Cardholder Data. Respondent should consider all information reasonably available to it in determining whether Hilton has a notification obligation to Consumers or the Attorney General under Vermont law. Lack of evidence of exfiltration, especially in cases where Respondent failed to collect, or otherwise deleted relevant forensic evidence, such as server images, malware output files, or log files, shall not be determinative. This determination will be a fact specific inquiry.

30. For a period of 5 years, if Respondent retains a PFI to investigate a breach involving Cardholder Data, it will provide notice of the breach incident that is being

investigated to the Attorney General as well as a copy of the PFI preliminary incident report. Notice shall be provided to the Attorney General within 14 days of retaining a PFI and the report will be provided within 10 days of issuance. The Attorney General shall treat the PFI preliminary incident report as confidential as if it were a notice submitted in accordance with 9 V.S.A. § 2435(b)(3)(B), which prohibits release of the notice under FOIA or Vermont's Public Records Law. All copies of the PFI preliminary incident report in the possession of the Attorney General's Office shall be destroyed by the Office if Hilton provides evidence that the breach did not involve the Cardholder Data of Vermont residents.

Comprehensive Information Security Program

31. Respondent shall design and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of Cardholder Data that it collects, receives or processes. Such program must be documented in writing, shall be appropriate to Respondent's size, complexity, the nature and scope of its activities, and the sensitivity of the data at issue, and have the following administrative, technical, and physical safeguards:

(a) the designation of an employee or employees to coordinate and be accountable for the information security program;

(b) the identification of material internal and external risks to the security, confidentiality, and integrity of Cardholder Data that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks;

(c) the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

(d) the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding Cardholder Data and requiring such service providers by contract to implement and maintain appropriate safeguards for such information; and

(e) the evaluation and adjustment of Respondent's information security program described herein in light of the results of the testing or monitoring required by sub-part (c) or any other circumstances (including any material changes to Respondent's operations or business arrangements) that Respondent knows or a reasonable entity acting objectively under the circumstances would know may have a material impact on the effectiveness of such information security program.

32. Respondent may comply with the requirements of Paragraph 31 through the use of compensating controls that meet the purpose and effectiveness of the controls described in Paragraph 31. If, at any time after the execution of this Assurance, Respondent believes that any of the specific prohibitions or affirmative obligations imposed by this Assurance should be altered on account of changes in technology or the law, it may request agreement to such amendment from the Attorney General.

Cardholder Data Assessments

33. Respondent shall annually obtain a written assessment of the extent of its compliance with the PCI DSS Requirements and Security Assessment Procedures, Version 3.2, attached hereto, or, in the event such standard no longer exists, any successor standard

established or approved by the PCI DSS Council, any successor entity to said Council, or all of the major payment card brands. For each annual assessment, the assessor conducting the assessment must certify as to the extent of Respondent's compliance with PCI DSS. As part of the assessment, the assessor must:

(a) certify that Respondent treats untrusted networks in accordance with PCI DSS Requirement No. 1.2 or its equivalent in any successor versions of PCI DSS, and if networks are not treated as untrusted, certify such networks either are included in the assessment or have during the 12 months preceding the assessment separately been validated to be fully compliant with PCI DSS;

(b) certify as to the extent of Respondent's compliance with each element of a risk management protocol at least as thorough as Version 2.0 of the PCI DSS Risk Assessment Guidelines, attached hereto as Exhibit B; and

(c) certify that the assessment was conducted by a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession, adheres to professional and business ethics, performs all duties objectively, and is free from any conflicts of interest that might compromise the assessor's independent judgment in performing assessments. The assessor shall be a person qualified as a Qualified Security Assessor under PCI DSS ("QSA"), or, at the election of Respondent, a similarly qualified person or organization approved by the Attorney General.

34. For a period of 5 years, if the assessor that conducts an assessment described in Paragraph 33 does not certify that Respondent is fully compliant with PCI DSS and with the risk protocol, Respondent shall notify the Attorney General immediately in writing,

outlining the deficiencies and reasons for the deficiencies, and remedy any deficiencies and obtain another certification confirming compliance within ninety (90) days from the completion of the noncompliant assessment or the risk protocol. Failure to fulfill the terms of this paragraph shall be considered a violation of this Assurance, unless otherwise agreed to by the parties.

IV. PENALTIES

35. Respondent shall pay the State civil penalties of Three Hundred Thousand Dollars ($300,000), within ten days of both Parties signing this Assurance. Respondent shall make payment to the "State of Vermont" and send payment to: Ryan Kriger, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609.

V. REPORTING

36. For a period of 5 years, to the extent not already provided under this Assurance, Respondent shall, upon request by Attorney General provide all documentation and information necessary for the requesting party to verify compliance with this Assurance.

37. For a period of 5 years, Respondent shall maintain all materials relied upon to prepare any assessment required by this Assurance for a period of three years after the assessment, whether prepared by or on behalf of Respondent, including but not limited to all reports, studies, reviews, audits, audit trails, policies, training materials and any other materials relied on to prepare the assessments.

VI. MISCELLANEOUS PROVISIONS

38. Respondent does not admit that it has violated Vermont law, and nothing

herein shall be deemed an admission or waiver of any right of Respondent.

39. Respondent does not admit to the allegations contained in Paragraphs 11, 12, 17, and 21.

40. This Assurance is not intended for use by any third party in any other proceeding and is not intended, and should not be construed, as an admission of liability by Respondent.

41. As of the Effective Date, the Plaintiff hereby releases Respondent from all civil claims, actions, causes of action, damages, losses, fines, costs, and penalties related to the allegations of the Assurance in this action, that have been or could have been brought against Respondent or any of its respective current or former affiliates, agents, representatives, or employees pursuant to the State of Vermont's Security Breach Notice Act, 9 V.S.A. Chapter 22, Consumer Protection Act, 9 V.S.A. Chapter 63 or civil fraud laws (including common law claims concerning fraudulent trade practices) on or before the Effective Date. Notwithstanding any other term of this Assurance, the following do not comprise Released Claims: private rights of action; criminal claims; claims of environmental or tax liability; claims for property damage; claims alleging violations of State or federal securities laws; claims alleging violations of State or federal antitrust laws; claims alleging violations of State or federal false claims laws; claims brought by any other agency or subdivision of the State; and claims alleging a breach of this Assurance.

42. The Parties agree that this Assurance does not constitute an approval by the Attorney General of any of Respondent's past or future practices, and Respondents shall not make any representation to the contrary.

43. The requirements of this Assurance are in addition to, and not in lieu of, any other requirements of state or federal law. Nothing in this Assurance shall be construed as relieving Respondent of the obligation to comply with all local, state, and federal laws, regulations, or rules, nor shall any of the provisions of this Assurance be deemed as permission for Respondent to engage in any acts or practices prohibited by such laws, regulations, or rules.

44. Respondent shall not participate directly or indirectly in any activity to form or proceed as a separate entity or corporation for the purpose of engaging in acts prohibited in this Assurance or for any other purpose which would otherwise circumvent any part of this Assurance.

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 other provision had not been contained herein.

46. The section headings and subheadings contained in this Assurance are included for convenience of reference only and shall be ignored in the construction or interpretation of this Assurance.

47. In the event that any statute, rule, or regulation pertaining to the subject matter of this Judgment is enacted, promulgated, modified, or interpreted by any federal or state government or agency, or a court of competent jurisdiction holds that such statute, rule, or regulation is in conflict with any provision of the Assurance, and compliance with the Assurance and the subject statute, rule or regulation is impossible, Respondent may

comply with such statute, rule or regulation and such action in the affected jurisdiction shall not constitute a violation of this Assurance. Respondent shall provide written notices to the Attorney General that it is impossible to comply with the Assurance and the subject law and shall explain in detail the basis for claimed impossibility, with specific reference to any applicable statutes, regulations, rules, and court opinions. Such notice shall be provided immediately upon Respondent learning of the potential impossibility and at least thirty (30) days in advance of any act or omission which is not in compliance with this Assurance. Nothing in this paragraph shall limit the right of the Attorney General to disagree with Respondent as to the impossibility of compliance and to seek to enforce this Assurance accordingly.

48. All notices under this Assurance shall be provided to the following via email and Overnight Mail:

For Hilton:

Office of the General Counsel
Hilton
7930 Jones Branch Drive
McLean, VA 22102

For the State of Vermont:

Ryan Kriger
Assistant Attorney General
Vermont Attorney General's Office
109 State Street
Montpelier, VT 05609
ryan.kriger@vermont.gov

49. This court retains jurisdiction of this action for the purpose of ensuring compliance with this Assurance.

APPROVED:

FOR RESPONDENT Hilton

By: _____ Date: 10/13/17
Michael Leffinger
Senior Vice President

FOR THE STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: _____ Date: 10/31/2017
Ryan Kriger
Assistant Attorney General

Exhibit A

Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures

Version 3.2
April 2016

Document Changes

Date	Version	Description	Pages
October 2008	1.2	To introduce PCI DSS v1.2 as "PCI DSS Requirements and Security Assessment Procedures," eliminating redundancy between documents, and make both general and specific changes from PCI DSS Security Audit Procedures v1.1. For complete information, see PCI Data Security Standard Summary of Changes from PCI DSS Version 1.1 to 1.2.	
July 2009	1.2.1	Add sentence that was incorrectly deleted between PCI DSS v1.1 and v1.2.	5
		Correct "then" to "than" in testing procedures 6.3.7.a and 6.3.7.b.	32
		Remove grayed-out marking for "in place" and "not in place" columns in testing procedure 6.5.b.	33
		For Compensating Controls Worksheet – Completed Example, correct wording at top of page to say "Use this worksheet to define compensating controls for any requirement noted as 'in place' via compensating controls."	64
October 2010	2.0	Update and implement changes from v1.2.1. See *PCI DSS – Summary of Changes from PCI DSS Version 1.2.1 to 2.0.*	
November 2013	3.0	Update from v2.0. See *PCI DSS – Summary of Changes from PCI DSS Version 2.0 to 3.0.*	
April 2015	3.1	Update from PCI DSS v3.0. See *PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1* for details of changes.	
April 2016	3.2	Update from PCI DSS v3.1. See *PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2* for details of changes.	

Table of Contents

Introduction and PCI Data Security Standard Overview

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to ***all*** entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to ***all*** other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD). Below is a high-level overview of the 12 PCI DSS requirements.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

This document, *PCI Data Security Standard Requirements and Security Assessment Procedures*, combines the 12 PCI DSS requirements and corresponding testing procedures into a security assessment tool. It is designed for use during PCI DSS compliance assessments as part of an entity's validation process. The following sections provide detailed guidelines and best practices to assist entities prepare for, conduct, and report the results of a PCI DSS assessment. The PCI DSS Requirements and Testing Procedures begin on page 15.

PCI DSS comprises a minimum set of requirements for protecting account data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personal information or other data elements (for example, cardholder name). PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements.

PCI DSS Resources

The PCI Security Standards Council (PCI SSC) website (www.pcisecuritystandards.org) contains a number of additional resources to assist organizations with their PCI DSS assessments and validations, including:

- Document Library, including:
  - *PCI DSS – Summary of Changes from PCI DSS version 2.0 to 3.0*
  - *PCI DSS Quick Reference Guide*
  - *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*
  - *Information Supplements and Guidelines*
  - *Prioritized Approach for PCI DSS*
  - *Report on Compliance (ROC) Reporting Template and Reporting Instructions*
  - *Self-assessment Questionnaires (SAQs) and SAQ Instructions and Guidelines*
  - *Attestations of Compliance (AOCs)*
- Frequently Asked Questions (FAQs)
- PCI for Small Merchants website
- PCI training courses and informational webinars
- List of Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs)
- List of PTS approved devices and PA-DSS validated payment applications

***Note**: Information Supplements complement the PCI DSS and identify additional considerations and recommendations for meeting PCI DSS requirements—they do not supersede, replace or extend the PCI DSS or any of its requirements.*

Please refer to *www.pcisecuritystandards.org* for information about these and other resources.

PCI DSS Applicability Information

PCI DSS applies to ***all*** entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to ***all*** other entities that store, process, or transmit cardholder data and/or sensitive authentication data.

Cardholder data and sensitive authentication data are defined as follows:

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
▪ Primary Account Number (PAN) ▪ Cardholder Name ▪ Expiration Date ▪ Service Code	▪ Full track data (magnetic-stripe data or equivalent on a chip) ▪ CAV2/CVC2/CVV2/CID ▪ PINs/PIN blocks

The primary account number is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment (CDE), they must be protected in accordance with applicable PCI DSS requirements.

PCI DSS requirements apply to organizations where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted. Some PCI DSS requirements may also be applicable to organizations that have outsourced their payment operations or management of their CDE[1]. Additionally, organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the account data is protected by the third party per the applicable PCI DSS requirements.

The table on the following page illustrates commonly used elements of cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited, and whether each data element must be protected. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

[1] In accordance with individual payment brand compliance programs

		Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[2]	Full Track Data[3]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID[4]	No	Cannot store per Requirement 3.2
		PIN/PIN Block[5]	No	Cannot store per Requirement 3.2

PCI DSS Requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.

Sensitive authentication data must not be stored after authorization, even if encrypted. This applies even where there is no PAN in the environment. Organizations should contact their acquirer or the individual payment brands directly to understand whether SAD is permitted to be stored prior to authorization, for how long, and any related usage and protection requirements.

---

2 Sensitive authentication data must not be stored after authorization (even if encrypted).
3 Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere
4 The three- or four-digit value printed on the front or back of a payment card
5 Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message

Relationship between PCI DSS and PA-DSS

Applicability of PCI DSS to PA-DSS Applications

Use of a Payment Application Data Security Standard (PA-DSS) compliant application by itself does not make an entity PCI DSS compliant, since that application must be implemented into a PCI DSS compliant environment and according to the PA-DSS Implementation Guide provided by the payment application vendor.

All applications that store, process, or transmit cardholder data are in scope for an entity's PCI DSS assessment, including applications that have been validated to PA-DSS. The PCI DSS assessment should verify the PA-DSS validated payment application is properly configured and securely implemented per PCI DSS requirements. If the payment application has undergone any customization, a more in-depth review will be required during the PCI DSS assessment, as the application may no longer be representative of the version that was validated to PA-DSS.

The PA-DSS requirements are derived from the *PCI DSS Requirements and Security Assessment Procedures* (defined in this document). The PA-DSS details the requirements a payment application must meet in order to facilitate a customer's PCI DSS compliance. As security threats are constantly evolving, applications that are no longer supported by the vendor (e.g., identified by the vendor as "end of life") may not offer the same level of security as supported versions.

Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of PAN, full track data, card verification codes and values (CAV2, CID, CVC2, CVV2), and PINs and PIN blocks, along with the damaging fraud resulting from these breaches.

To determine whether PA-DSS applies to a given payment application, please refer to the PA-DSS Program Guide, which can be found at www.pcisecuritystandards.org.

Applicability of PCI DSS to Payment Application Vendors

PCI DSS may apply to payment application vendors if the vendor stores, processes, or transmits cardholder data, or has access to their customers' cardholder data (for example, in the role of a service provider).

Scope of PCI DSS Requirements

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications. Examples of system components include but are not limited to the following:

- Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the CDE.
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Network components including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- Applications including all purchased and custom applications, including internal and external (for example, Internet) applications.
- Any other component or device located within or connected to the CDE.

The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers) to ensure they are included in the PCI DSS scope. All types of systems and locations should be considered as part of the scoping process, including backup/recovery sites and fail-over systems.

To confirm the accuracy of the defined CDE, perform the following:

- The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined CDE.
- Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).
- The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE. If the entity identifies data that is not currently included in the CDE, such data should be securely deleted, migrated into the currently defined CDE, or the CDE redefined to include this data.

The entity retains documentation that shows how PCI DSS scope was determined. The documentation is retained for assessor review and/or for reference during the next annual PCI DSS scope confirmation activity.

For each PCI DSS assessment, the assessor is required to validate that the scope of the assessment is accurately defined and documented.

Network Segmentation

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce:

- The scope of the PCI DSS assessment
- The cost of the PCI DSS assessment
- The cost and difficulty of implementing and maintaining PCI DSS controls
- The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)

Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment. Network segmentation can be achieved through a number of physical or logical means, such as properly configured internal network firewalls, routers with strong access control lists, or other technologies that restrict access to a particular segment of a network. To be considered out of scope for PCI DSS, a system component must be properly isolated (segmented) from the CDE, such that even if the out-of-scope system component was compromised it could not impact the security of the CDE.

An important prerequisite to reduce the scope of the cardholder data environment is a clear understanding of business needs and processes related to the storage, processing or transmission of cardholder data. Restricting cardholder data to as few locations as possible by elimination of unnecessary data, and consolidation of necessary data, may require reengineering of long-standing business practices.

Documenting cardholder data flows via a dataflow diagram helps fully understand all cardholder data flows and ensures that any network segmentation is effective at isolating the cardholder data environment.

If network segmentation is in place and being used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment. At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not. However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon a number of factors, such as a given network's configuration, the technologies deployed, and other controls that may be implemented.

Appendix D: Segmentation and Sampling of Business Facilities/System Components provides more information on the effect of network segmentation and sampling on the scope of a PCI DSS assessment.

Wireless

If wireless technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, "line-busting"), or if a wireless local area network (WLAN) is part of, or connected to the cardholder data environment, the PCI DSS requirements and testing procedures for wireless environments apply and must be performed (for example, Requirements 1.2.3, 2.1.1, and 4.1.1). Before wireless technology is implemented, an entity should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.

Use of Third-Party Service Providers / Outsourcing

A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.

Parties should clearly identify the services and system components which are included in the scope of the service provider's PCI DSS assessment, the specific PCI DSS requirements covered by the service provider, and any requirements which are the responsibility of the service provider's customers to include in their own PCI DSS reviews. For example, a managed hosting provider should clearly define which of their IP addresses are scanned as part of their quarterly vulnerability scan process and which IP addresses are their customer's responsibility to include in their own quarterly scans.

Service providers are responsible for demonstrating their PCI DSS compliance, and may be required to do so by the payment brands. Service providers should contact their acquirer and/or payment brand to determine the appropriate compliance validation.

There are two options for third-party service providers to validate compliance:

1) **Annual assessment**: Service providers can undergo an annual PCI DSS assessment(s) on their own and provide evidence to their customers to demonstrate their compliance; or
2) **Multiple, on-demand assessments**: If they do not undergo their own annual PCI DSS assessments, service providers must undergo assessments upon request of their customers and/or participate in each of their customer's PCI DSS reviews, with the results of each review provided to the respective customer(s)

If the third party undergoes their own PCI DSS assessment, they should provide sufficient evidence to their customers to verify that the scope of the service provider's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place. The specific type of evidence provided by the service provider to their customers will depend on the agreements/contracts in place between those parties. For example, providing the AOC and/or relevant sections of the service provider's ROC (redacted to protect any confidential information) could help provide all or some of the information.

Additionally, merchants and service providers must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data. *Refer to Requirement 12.8 in this document for details.*

Best Practices for Implementing PCI DSS into Business-as-Usual Processes

To ensure security controls continue to be properly implemented, PCI DSS should be implemented into business-as-usual (BAU) activities as part of an entity's overall security strategy. This enables an entity to monitor the effectiveness of their security controls on an ongoing basis, and maintain their PCI DSS compliant environment in between PCI DSS assessments. Examples of how to incorporate PCI DSS into BAU activities include but are not limited to:

1. Monitoring of security controls—such as firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), file-integrity monitoring (FIM), anti-virus, access controls, etc.—to ensure they are operating effectively and as intended.
2. Ensuring that all failures in security controls are detected and responded to in a timely manner. Processes to respond to security control failures should include:
   - Restoring the security control
   - Identifying the cause of failure
   - Identifying and addressing any security issues that arose during the failure of the security control
   - Implementing mitigation (such as process or technical controls) to prevent the cause of the failure recurring
   - Resuming monitoring of the security control, perhaps with enhanced monitoring for a period of time, to verify the control is operating effectively
3. Reviewing changes to the environment (for example, addition of new systems, changes in system or network configurations) prior to completion of the change, and perform the following:
   - Determine the potential impact to PCI DSS scope (for example, a new firewall rule that permits connectivity between a system in the CDE and another system could bring additional systems or networks into scope for PCI DSS).
   - Identify PCI DSS requirements applicable to systems and networks affected by the changes (for example, if a new system is in scope for PCI DSS, it would need to be configured per system configuration standards, including FIM, AV, patches, audit logging, etc., and would need to be added to the quarterly vulnerability scan schedule).
   - Update PCI DSS scope and implement security controls as appropriate.
4. Changes to organizational structure (for example, a company merger or acquisition) resulting in formal review of the impact to PCI DSS scope and requirements.
5. Performing periodic reviews and communications to confirm that PCI DSS requirements continue to be in place and personnel are following secure processes. These periodic reviews should cover all facilities and locations, including retail outlets, data centers, etc., and include reviewing system components (or samples of system components), to verify that PCI DSS requirements continue to be in place—for example, configuration standards have been applied, patches and AV are up to date, audit logs are being reviewed, and so on. The frequency of periodic reviews should be determined by the entity as appropriate for the size and complexity of their environment.

   These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity's preparation for their next compliance assessment.

6. Reviewing hardware and software technologies at least annually to confirm that they continue to be supported by the vendor and can meet the entity's security requirements, including PCI DSS. If it is discovered that technologies are no longer supported by the vendor or cannot meet the entity's security needs, the entity should prepare a remediation plan, up to and including replacement of the technology, as necessary.

In addition to the above practices, organizations may also wish to consider implementing separation of duties for their security functions so that security and/or audit functions are separated from operational functions. In environments where one individual performs multiple roles (for example, administration and security operations), duties may be assigned such that no single individual has end-to-end control of a process without an independent checkpoint. For example, responsibility for configuration and responsibility for approving changes could be assigned to separate individuals.

Note: *For some entities, these best practices are also requirements to ensure ongoing PCI DSS compliance. For example, PCI DSS includes these principles in some requirements, and the Designated Entities Supplemental Validation (PCI DSS Appendix A3) requires designated entities to validate to these principles.*

All organizations should consider implementing these best practices into their environment, even where the organization is not required to validate to them.

For Assessors: Sampling of Business Facilities/System Components

Sampling is an option for assessors to facilitate the assessment process where there are large numbers of business facilities and/or system components.

While it is acceptable for an assessor to sample business facilities/system components as part of their review of an entity's PCI DSS compliance, it is not acceptable for an entity to apply PCI DSS requirements to only a sample of their environment (for example, requirements for quarterly vulnerability scans apply to all system components). Similarly, it is not acceptable for an assessor to only review a sample of PCI DSS requirements for compliance.

After considering the overall scope and complexity of the environment being assessed, the assessor may independently select representative samples of business facilities/system components in order to assess the entity's compliance with PCI DSS requirements. These samples must be defined first for business facilities and then for system components within each selected business facility. Samples must be a representative selection of all of the types and locations of business facilities, as well as all of the types of system components within selected business facilities. Samples must be sufficiently large to provide the assessor with assurance that controls are implemented as expected.

Examples of business facilities include but are not limited to: corporate offices, stores, franchise locations, processing facilities, data centers, and other facility types in different locations. Sampling should include system components within each selected business facility. For example, for each business facility selected, include a variety of operating systems, functions, and applications that are applicable to the area under review.

As an example, the assessor may define a sample at a business facility to include Sun servers running Apache, Windows servers running Oracle, mainframe systems running legacy card processing applications, data-transfer servers running HP-UX, and Linux Servers running MySQL. If all applications run from a single version of an OS (for example, Windows 7 or Solaris 10), the sample should still include a variety of applications (for example, database servers, web servers, data-transfer servers).

When independently selecting samples of business facilities/system components, assessors should consider the following:

- If there are standardized, centralized PCI DSS security and operational processes and controls in place that ensure consistency and that each business facility/system component must follow, the sample can be smaller than if there are no standard processes/controls in place. The sample must be large enough to provide the assessor with reasonable assurance that all business facilities/system components are configured per the standard processes. The assessor must verify that the standardized, centralized controls are implemented and working effectively.
- If there is more than one type of standard security and/or operational process in place (for example, for different types of business facilities/system components), the sample must be large enough to include business facilities/system components secured with each type of process.
- If there are no standard PCI DSS processes/controls in place and each business facility/system component is managed through non-standard processes, the sample must be larger for the assessor to be assured that each business facility/system component has implemented PCI DSS requirements appropriately.

- Samples of system components must include every type and combination that is in use. For example, where applications are sampled, the sample must include all versions and platforms for each type of application.

For each instance where sampling is used, the assessor must:

- Document the rationale behind the sampling technique and sample size,
- Document and validate the standardized PCI DSS processes and controls used to determine sample size, and
- Explain how the sample is appropriate and representative of the overall population.

Please also refer to:
Appendix D: Segmentation and Sampling of Business Facilities/System Components.

Assessors must revalidate the sampling rationale for each assessment. If sampling is to be used, different samples of business facilities and system components must be selected for each assessment.

Compensating Controls

On an annual basis, any compensating controls must be documented, reviewed and validated by the assessor and included with the Report on Compliance submission, per *Appendix B: Compensating Controls* and *Appendix C: Compensating Controls Worksheet.*

For each and every compensating control, the Compensating Controls Worksheet *(Appendix C)* **must** be completed. Additionally, compensating control results should be documented in the ROC in the corresponding PCI DSS requirement section.

See the above-mentioned *Appendices B* and *C* for more details on "compensating controls."

Instructions and Content for Report on Compliance

Instructions and content for the Report on Compliance (ROC) are provided in the *PCI DSS ROC Reporting Template*.

The *PCI DSS ROC Reporting Template* must be used as the template for creating the *Report on Compliance*. The assessed entity should follow each payment brand's respective reporting requirements to ensure each payment brand acknowledges the entity's compliance status. Contact each payment brand or the acquirer to determine reporting requirements and instructions.

PCI DSS Assessment Process

The PCI DSS assessment process includes completion of the following steps:

1. Confirm the scope of the PCI DSS assessment.
2. Perform the PCI DSS assessment of the environment, following the testing procedures for each requirement.
3. Complete the applicable report for the assessment (i.e., Self-*Assessment Questionnaire* (SAQ) or Report on Compliance (ROC)), including documentation of all compensating controls, according to the applicable PCI guidance and instructions.
4. Complete the Attestation of Compliance for Service Providers or Merchants, as applicable, in its entirety. Attestations of Compliance are available on the PCI SSC website.
5. Submit the SAQ or ROC, and the Attestation of Compliance, along with any other requested documentation—such as ASV scan reports—to the acquirer (for merchants) or to the payment brand or other requester (for service providers).
6. If required, perform remediation to address requirements that are not in place, and provide an updated report.

PCI DSS Versions

As of the published date of this document, PCI DSS v3.1 is valid until October 31, 2016, after which it is retired. All PCI DSS validations after this date must be to PCI DSS v3.2 or later.

The following table provides a summary of PCI DSS versions and their effective dates[6].

Version	Published	Retired
PCI DSS v3.2 (This document)	April 2016	To be determined
PCI DSS v3.1	April 2015	October 31, 2016

[6] Subject to change upon release of a new version of PCI DSS.

Detailed PCI DSS Requirements and Security Assessment Procedures

The following defines the column headings for the PCI DSS Requirements and Security Assessment Procedures:

- **PCI DSS Requirements** – This column defines the Data Security Standard requirements; PCI DSS compliance is validated against these requirements.
- **Testing Procedures** – This column shows processes to be followed by the assessor to validate that PCI DSS requirements have been met and are "in place."
- **Guidance** – This column describes the intent or security objective behind each of the PCI DSS requirements. This column contains guidance only, and is intended to assist understanding of the intent of each requirement. The guidance in this column does not replace or extend the PCI DSS Requirements and Testing Procedures.

Note: *PCI DSS requirements are not considered to be in place if controls are not yet implemented or are scheduled to be completed at a future date. After any open or not-in-place items are addressed by the entity, the assessor will then reassess to validate that the remediation is completed and that all requirements are satisfied.*

Please refer to the following resources (available on the PCI SSC website) to document the PCI DSS assessment:

- *For instructions on completing reports on compliance (ROC), refer to the* PCI DSS ROC Reporting Template.
- *For instructions on completing self-assessment questionnaires (SAQ), refer to the* PCI DSS SAQ Instructions and Guidelines.
- *For instructions on submitting PCI DSS compliance validation reports, refer to the* PCI DSS Attestations of Compliance.

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

PCI DSS Requirements	Testing Procedures	Guidance
1.1 Establish and implement firewall and router configuration standards that include the following:	**1.1** Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:	Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These devices are software or hardware devices that block unwanted access and manage authorized access into and out of the network. Configuration standards and procedures will help to ensure that the organization's first line of defense in the protection of its data remains strong.
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1.a** Examine documented procedures to verify there is a formal process for testing and approval of all: • Network connections and • Changes to firewall and router configurations	A documented and implemented process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall. Without formal approval and testing of changes, records of the changes might not be updated, which could lead to inconsistencies between network documentation and the actual configuration.
	1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	**1.1.2.a** Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	**1.1.3** Examine data-flow diagram and interview personnel to verify the diagram: • Shows all cardholder data flows across systems and networks. • Is kept current and updated as needed upon changes to the environment.	Cardholder data-flow diagrams identify the location of all cardholder data that is stored, processed, or transmitted within the network. Network and cardholder data-flow diagrams help an organization to understand and keep track of the scope of their environment, by showing how cardholder data flows across networks and between individual systems and devices.
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.4.a** Examine the firewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.	Using a firewall on every Internet connection coming into (and out of) the network, and between any DMZ and the internal network, allows the organization to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection.
	1.1.4.b Verify that the current network diagram is consistent with the firewall configuration standards.	
	1.1.4.c Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone, per the documented configuration standards and network diagrams.	

PCI DSS Requirements	Testing Procedures	Guidance
1.1.5 Description of groups, roles, and responsibilities for management of network components	**1.1.5.a** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.	This description of roles and assignment of responsibilities ensures that personnel are aware of who is responsible for the security of all network components, and that those assigned to manage components are aware of their responsibilities. If roles and responsibilities are not formally assigned, devices could be left unmanaged.
	1.1.5.b Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented.	
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	**1.1.6.a** Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each.	Compromises often happen due to unused or insecure service and ports, since these often have known vulnerabilities and many organizations don't patch vulnerabilities for the services, protocols, and ports they don't use (even though the vulnerabilities are still present). By clearly defining and documenting the services, protocols, and ports that are necessary for business, organizations can ensure that all other services, protocols, and ports are disabled or removed. Approvals should be granted by personnel independent of the personnel managing the configuration. If insecure services, protocols, or ports are necessary for business, the risk posed by use of these protocols should be clearly understood and accepted by the organization, the use of the protocol should be justified, and the security features that allow these protocols to be used securely should be documented and implemented. If these insecure services, protocols, or ports are not necessary for business, they should be disabled or removed. For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance (e.g., NIST, ENISA, OWASP, etc.).
	1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.	
	1.1.6.c Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port.	

PCI DSS Requirements	Testing Procedures	Guidance
1.1.7 Requirement to review firewall and router rule sets at least every six months	**1.1.7.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.	This review gives the organization an opportunity at least every six months to clean up any unneeded, outdated, or incorrect rules, and ensure that all rule sets allow only authorized services and ports that match the documented business justifications. Organizations with a high volume of changes to firewall and router rule sets may wish to consider performing reviews more frequently, to ensure that the rule sets continue to meet the needs of the business.
	1.1.7.b Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months.	
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	**1.2** Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the cardholder data environment:	It is essential to install network protection between the internal, trusted network and any untrusted network that is external and/or out of the entity's ability to control or manage. Failure to implement this measure correctly results in the entity being vulnerable to unauthorized access by malicious individuals or software. For firewall functionality to be effective, it must be properly configured to control and/or limit traffic into and out of the entity's network.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	**1.2.1.a** Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment.	Examination of all inbound and outbound connections allows for inspection and restriction of traffic based on the source and/or destination address, thus preventing unfiltered access between untrusted and trusted environments. This prevents malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within the entity's network out to an untrusted server). Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in or out.
	1.2.1.b Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.	
	1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.	

PCI DSS Requirements	Testing Procedures	Guidance
1.2.2 Secure and synchronize router configuration files.	**1.2.2.a** Examine router configuration files to verify they are secured from unauthorized access.	While the running (or active) router configuration files include the current, secure settings, the start-up files (which are used when routers are re-started or booted) must be updated with the same secure settings to ensure these settings are applied when the start-up configuration is run. Because they only run occasionally, start-up configuration files are often forgotten and are not updated. When a router re-starts and loads a start-up configuration that has not been updated with the same secure settings as those in the running configuration, it may result in weaker rules that allow malicious individuals into the network.
	1.2.2.b Examine router configurations to verify they are synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted).	
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	**1.2.3.a** Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the cardholder data environment.	The known (or unknown) implementation and exploitation of wireless technology within a network is a common path for malicious individuals to gain access to the network and cardholder data. If a wireless device or network is installed without the entity's knowledge, a malicious individual could easily and "invisibly" enter the network. If firewalls do not restrict access from wireless networks into the CDE, malicious individuals that gain unauthorized access to the wireless network can easily connect to the CDE and compromise account information. Firewalls must be installed between all wireless networks and the CDE, regardless of the purpose of the environment to which the wireless network is connected. This may include, but is not limited to, corporate networks, retail stores, guest networks, warehouse environments, etc.
	1.2.3.b Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	

PCI DSS Requirements	Testing Procedures	Guidance
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	**1.3** Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—and perform the following to determine that there is no direct access between the Internet and system components in the internal cardholder network segment:	While there may be legitimate reasons for untrusted connections to be permitted to DMZ systems (e.g., to allow public access to a web server), such connections should never be granted to systems in the internal network. A firewall's intent is to manage and control all connections between public systems and internal systems, especially those that store, process or transmit cardholder data. If direct access is allowed between public systems and the CDE, the protections offered by the firewall are bypassed, and system components storing cardholder data may be exposed to compromise.
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	**1.3.1** Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	The DMZ is that part of the network that manages connections between the Internet (or other untrusted networks), and services that an organization needs to have available to the public (like a web server). This functionality is intended to prevent malicious individuals from accessing the organization's internal network from the Internet, or from using services, protocols, or ports in an unauthorized manner.
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	**1.3.2** Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ.	
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	**1.3.3** Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ.	Normally a packet contains the IP address of the computer that originally sent it so other computers in the network know where the packet came from. Malicious individuals will often try to spoof (or imitate) the sending IP address so that the target system believes the packet is from a trusted source. Filtering packets coming into the network helps to, among other things, ensure packets are not "spoofed" to look like they are coming from an organization's own internal network.

PCI DSS Requirements	Testing Procedures	Guidance
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	**1.3.4** Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.	All traffic outbound from the cardholder data environment should be evaluated to ensure that it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications (for example by restricting source/destination addresses/ports, and/or blocking of content).
1.3.5 Permit only "established" connections into the network.	**1.3.5** Examine firewall and router configurations to verify that the firewall permits only established connections into the internal network and denies any inbound connections not associated with a previously established session.	A firewall that maintains the "state" (or the status) for each connection through the firewall knows whether an apparent response to a previous connection is actually a valid, authorized response (since it retains each connection's status) or is malicious traffic trying to trick the firewall into allowing the connection.
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	**1.3.6** Examine firewall and router configurations to verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.	If cardholder data is located within the DMZ, it is easier for an external attacker to access this information, since there are fewer layers to penetrate. Securing system components that store cardholder data in an internal network zone that is segregated from the DMZ and other untrusted networks by a firewall can prevent unauthorized network traffic from reaching the system component. ***Note:*** *This requirement is not intended to apply to temporary storage of cardholder data in volatile memory.*

PCI DSS Requirements	Testing Procedures	Guidance
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. ***Note:*** *Methods to obscure IP addressing may include, but are not limited to:* • *Network Address Translation (NAT)* • *Placing servers containing cardholder data behind proxy servers/firewalls,* • *Removal or filtering of route advertisements for private networks that employ registered addressing,* • *Internal use of RFC1918 address space instead of registered addresses.*	**1.3.7.a** Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.	Restricting the disclosure of internal or private IP addresses is essential to prevent a hacker "learning" the IP addresses of the internal network, and using that information to access the network. Methods used to meet the intent of this requirement may vary depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.
	1.3.7.b Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized.	

PCI DSS Requirements	Testing Procedures	Guidance
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	**1.4.a** Examine policies and configuration standards to verify: • Personal firewall software or equivalent functionality is required for all portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. • Specific configuration settings are defined for personal firewall (or equivalent functionality). • Personal firewall (or equivalent functionality) is configured to actively run. • Personal firewall (or equivalent functionality) is configured to not be alterable by users of the portable computing devices.	Portable computing devices that are allowed to connect to the Internet from outside the corporate firewall are more vulnerable to Internet-based threats. Use of firewall functionality (e.g., personal firewall software or hardware) helps to protect devices from Internet-based attacks, which could use the device to gain access the organization's systems and data once the device is re-connected to the network. The specific firewall configuration settings are determined by the organization. ***Note:*** *This requirement applies to employee-owned and company-owned portable computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit. Allowing untrusted systems to connect to an organization's CDE could result in access being granted to attackers and other malicious users.*
	1.4.b Inspect a sample of company and/or employee-owned devices to verify that: • Personal firewall (or equivalent functionality) is installed and configured per the organization's specific configuration settings. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	**1.5** Examine documentation and interview personnel to verify that security policies and operational procedures for managing firewalls are: • Documented, • In use, and • Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures to ensure firewalls and routers are continuously managed to prevent unauthorized access to the network.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI DSS Requirements	Testing Procedures	Guidance
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	**2.1.a** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)	Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.
	2.1.b For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled.	
	2.1.c Interview personnel and examine supporting documentation to verify that: • All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. • Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network.	

PCI DSS Requirements	Testing Procedures	Guidance
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	**2.1.1.a** Interview responsible personnel and examine supporting documentation to verify that: • Encryption keys were changed from default at installation • Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions.	If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network. In addition, the key-exchange protocol for older versions of 802.11x encryption (Wired Equivalent Privacy, or WEP) has been broken and can render the encryption useless. Firmware for devices should be updated to support more secure protocols.
	2.1.1.b Interview personnel and examine policies and procedures to verify: • Default SNMP community strings are required to be changed upon installation. • Default passwords/passphrases on access points are required to be changed upon installation.	
	2.1.1.c Examine vendor documentation and login to wireless devices, with system administrator help, to verify: • Default SNMP community strings are not used. • Default passwords/passphrases on access points are not used.	
	2.1.1.d Examine vendor documentation and observe wireless configuration settings to verify firmware on wireless devices is updated to support strong encryption for: • Authentication over wireless networks • Transmission over wireless networks.	
	2.1.1.e Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.	

PCI DSS Requirements	Testing Procedures	Guidance
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	**2.2.a** Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards. **2.2.b** Examine policies and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1. **2.2.c** Examine policies and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network. **2.2.d** Verify that system configuration standards include the following procedures for all types of system components: • Changing of all vendor-supplied defaults and elimination of unnecessary default accounts • Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server • Enabling only necessary services, protocols, daemons, etc., as required for the function of the system • Implementing additional security features for any required services, protocols or daemons that are considered to be insecure • Configuring system security parameters to prevent misuse • Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	There are known weaknesses with many operating systems, databases, and enterprise applications, and there are also known ways to configure these systems to fix security vulnerabilities. To help those that are not security experts, a number of security organizations have established system-hardening guidelines and recommendations, which advise how to correct these weaknesses. Examples of sources for guidance on configuration standards include, but are not limited to: www.nist.gov, www.sans.org, and www.cisecurity.org, www.iso.org, and product vendors. System configuration standards must be kept up to date to ensure that newly identified weaknesses are corrected prior to a system being installed on the network.

PCI DSS Requirements	Testing Procedures	Guidance
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) ***Note:*** *Where virtualization technologies are in use, implement only one primary function per virtual system component.*	**2.2.1.a** Select a sample of system components and inspect the system configurations to verify that only one primary function is implemented per server. **2.2.1.b** If virtualization technologies are used, inspect the system configurations to verify that only one primary function is implemented per virtual system component or device.	If server functions that need different security levels are located on the same server, the security level of the functions with higher security needs would be reduced due to the presence of the lower-security functions. Additionally, the server functions with a lower security level may introduce security weaknesses to other functions on the same server. By considering the security needs of different server functions as part of the system configuration standards and related processes, organizations can ensure that functions requiring different security levels don't co-exist on the same server.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	**2.2.2.a** Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled. **2.2.2.b** Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards.	As stated in Requirement 1.1.6, there are many protocols that a business may need (or have enabled by default) that are commonly used by malicious individuals to compromise a network. Including this requirement as part of an organization's configuration standards and related processes ensures that only the necessary services and protocols are enabled.
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	**2.2.3.a** Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols. **2.2.3.b** If SSL/early TLS is used, perform testing procedures in *Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.*	Enabling security features before new servers are deployed will prevent servers being installed into the environment with insecure configurations. Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to take advantage of commonly used points of compromise within a network. Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.).

PCI DSS Requirements	Testing Procedures	Guidance
2.2.4 Configure system security parameters to prevent misuse.	**2.2.4.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.	System configuration standards and related processes should specifically address security settings and parameters that have known security implications for each type of system in use. In order for systems to be configured securely, personnel responsible for configuration and/or administering systems must be knowledgeable in the specific security parameters and settings that apply to the system.
	2.2.4.b Examine the system configuration standards to verify that common security parameter settings are included.	
	2.2.4.c Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards.	
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**2.2.5.a** Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.	Unnecessary functions can provide additional opportunities for malicious individuals to gain access to a system. By removing unnecessary functionality, organizations can focus on securing the functions that are required and reduce the risk that unknown functions will be exploited. Including this in server-hardening standards and processes addresses the specific security implications associated with unnecessary functions (for example, by removing/disabling FTP or the web server if the server will not be performing those functions).
	2.2.5.b. Examine the documentation and security parameters to verify enabled functions are documented and support secure configuration.	
	2.2.5.c. Examine the documentation and security parameters to verify that only documented functionality is present on the sampled system components.	

PCI DSS Requirements	Testing Procedures	Guidance
2.3 Encrypt all non-console administrative access using strong cryptography. ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	**2.3** Select a sample of system components and verify that non-console administrative access is encrypted by performing the following:	If non-console (including remote) administration does not use secure authentication and encrypted communications, sensitive administrative or operational level information (like administrator's IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data. Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information. To be considered "strong cryptography," industry-recognized protocols with appropriate key strengths and key management should be in place as applicable for the type of technology in use. (Refer to "strong cryptography" in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms,* and industry standards and best practices such as NIST SP 800-52 and SP 800-57, OWASP, etc.)
	2.3.a Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator's password is requested.	
	2.3.b Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.	
	2.3.c Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography.	
	2.3.d Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.	
	2.3.e If SSL/early TLS is used, perform testing procedures in *Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.*	
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	**2.4.a** Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each.	Maintaining a current list of all system components will enable an organization to accurately and efficiently define the scope of their environment for implementing PCI DSS controls. Without an inventory, some system components could be forgotten, and be inadvertently excluded from the organization's configuration standards.
	2.4.b Interview personnel to verify the documented inventory is kept current.	

PCI DSS Requirements	Testing Procedures	Guidance
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**2.5** Examine documentation and interview personnel to verify that security policies and operational procedures for managing vendor defaults and other security parameters are: • Documented, • In use, and • Known to all affected parties.	Personnel need to be aware of and following security policies and daily operational procedures to ensure vendor defaults and other security parameters are continuously managed to prevent insecure configurations.
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.*	**2.6** Perform testing procedures **A1.1** through **A1.4** detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.	This is intended for hosting providers that provide shared hosting environments for multiple clients on the same server. When all data is on the same server and under control of a single environment, often the settings on these shared servers are not manageable by individual clients. This allows clients to add insecure functions and scripts that impact the security of all other client environments; and thereby make it easy for a malicious individual to compromise one client's data and thereby gain access to all other clients' data. See *Appendix A1* for details of requirements.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography" and other PCI DSS terms.

PCI DSS Requirements	Testing Procedures	Guidance
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	**3.1.a** Examine the data retention and disposal policies, procedures and processes to verify they include the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. • Specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons). • Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons. • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.	A formal data retention policy identifies what data needs to be retained, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. The only cardholder data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code. Understanding where cardholder data is located is necessary so it can be properly retained or disposed of when no longer needed. In order to define appropriate retention requirements, an entity first needs to understand their own business needs as well as any legal or regulatory obligations that apply to their industry, and/or that apply to the type of data being retained.
	3.1.b Interview personnel to verify that: • All locations of stored cardholder data are included in the data retention and disposal processes. • Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. • The quarterly automatic or manual process is performed for all locations of cardholder data.	

(Continued on next page)

PCI DSS Requirements	Testing Procedures	Guidance
	3.1.c For a sample of system components that store cardholder data: • Examine files and system records to verify that the data stored does not exceed the requirements defined in the data retention policy • Observe the deletion mechanism to verify data is deleted securely.	Identifying and deleting stored data that has exceeded its specified retention period prevents unnecessary retention of data that is no longer needed. This process may be automated or manual or a combination of both. For example, a programmatic procedure (automatic or manual) to locate and remove data and/or a manual review of data storage areas could be performed. Implementing secure deletion methods ensure that the data cannot be retrieved when it is no longer needed. ***Remember, if you don't need it, don't store it!***
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:* • *There is a business justification and* • *The data is stored securely.* Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	**3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data. **3.2.b** For issuers and/or companies that support issuing services and store sensitive authentication data, examine data stores and system configurations to verify that the sensitive authentication data is secured. **3.2.c** For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization.	Sensitive authentication data consists of full track data, card validation code or value, and PIN data. Storage of sensitive authentication data after authorization is prohibited! This data is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions. Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data. It should be noted that all PCI DSS requirements apply to issuers, and the only exception for issuers and issuer processors is that sensitive authentication data may be retained if there is a legitimate reason to do so. A legitimate reason is one that is necessary for the performance of the function being provided for the issuer and not one of convenience. Any such data must be stored securely and in accordance with all PCI DSS and specific payment brand requirements. *(Continued on next page)*

PCI DSS Requirements	Testing Procedures	Guidance
	3.2.d For all other entities, if sensitive authentication data is received, review procedures and examine the processes for securely deleting the data to verify that the data is unrecoverable.	For non-issuing entities, retaining sensitive authentication data post-authorization is not permitted.
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name* • *Primary account number (PAN)* • *Expiration date* • *Service code* *To minimize risk, store only these data elements as needed for business.*	**3.2.1** For a sample of system components, examine data sources including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents.	If full track data is stored, malicious individuals who obtain that data can use it to reproduce payment cards and complete fraudulent transactions.
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.	**3.2.2** For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents.	The purpose of the card validation code is to protect "card-not-present" transactions—Internet or mail order/telephone order (MO/TO) transactions—where the consumer and the card are not present. If this data is stolen, malicious individuals can execute fraudulent Internet and MO/TO transactions.

PCI DSS Requirements	Testing Procedures	Guidance
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	**3.2.3** For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored after authorization: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents.	These values should be known only to the card owner or bank that issued the card. If this data is stolen, malicious individuals can execute fraudulent PIN-based debit transactions (for example, ATM withdrawals).
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. ***Note**: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*	**3.3.a** Examine written policies and procedures for masking the display of PANs to verify: • A list of roles that need access to displays of more than the first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access. • PAN must be masked when displayed such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. • All roles not specifically authorized to see the full PAN must only see masked PANs.	The display of full PAN on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that full PAN is only displayed for those with a legitimate business need to see the full PAN minimizes the risk of unauthorized persons gaining access to PAN data. The masking approach should always ensure that only the minimum number of digits is displayed as necessary to perform a specific business function. For example, if only the last four digits are needed to perform a business function, mask the PAN so that individuals performing that function can view only the last four digits. As another example, if a function needs access to the bank identification number (BIN) for routing purposes, unmask only the BIN digits (traditionally the first six digits) during that function. This requirement relates to protection of PAN *displayed* on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.4 for protection of PAN when *stored* in files, databases, etc.
	3.3.b Examine system configurations to verify that full PAN is only displayed for users/roles with a documented business need, and that PAN is masked for all other requests.	
	3.3.c Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are able to see more than the first six/last four digits of the PAN.	

PCI DSS Requirements	Testing Procedures	Guidance
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	**3.4.a** Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods: • One-way hashes based on strong cryptography, • Truncation • Index tokens and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures. **3.4.b** Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text). **3.4.c** Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable. **3.4.d** Examine a sample of audit logs, including payment application logs, to confirm that PAN is rendered unreadable or is not present in the logs. **3.4.e** If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception or troubleshooting logs) must all be protected. One-way hash functions based on strong cryptography can be used to render cardholder data unreadable. Hash functions are appropriate when there is no need to retrieve the original number (one-way hashes are irreversible). It is recommended, but not currently a requirement, that an additional, random input value be added to the cardholder data prior to hashing to reduce the feasibility of an attacker comparing the data against (and deriving the PAN from) tables of pre-computed hash values. The intent of truncation is to permanently remove a segment of PAN data so that only a portion (generally not to exceed the first six and last four digits) of the PAN is stored. An index token is a cryptographic token that replaces the PAN based on a given index for an unpredictable value. A one-time pad is a system in which a randomly generated private key is used only once to encrypt a message that is then decrypted using a matching one-time pad and key. The intent of strong cryptography (as defined in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*) is that the encryption be based on an industry-tested and accepted algorithm (not a proprietary or "home-grown" algorithm) with strong cryptographic keys. By correlating hashed and truncated versions of a given PAN, a malicious individual may easily derive the original PAN value. Controls that prevent the correlation of this data will help ensure that the original PAN remains unreadable.

PCI DSS Requirements	Testing Procedures	Guidance
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. ***Note:*** *This requirement applies in addition to all other PCI DSS encryption and key-management requirements.*	**3.4.1.a** If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating system's authentication mechanism (for example, not using local user account databases or general network login credentials). **3.4.1.b** Observe processes and interview personnel to verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls). **3.4.1.c** Examine the configurations and observe the processes to verify that cardholder data on removable media is encrypted wherever stored. ***Note:*** *If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.*	The intent of this requirement is to address the acceptability of disk-level encryption for rendering cardholder data unreadable. Disk-level encryption encrypts the entire disk/partition on a computer and automatically decrypts the information when an authorized user requests it. Many disk-encryption solutions intercept operating system read/write operations and carry out the appropriate cryptographic transformations without any special action by the user other than supplying a password or pass phrase upon system startup or at the beginning of a session. Based on these characteristics of disk-level encryption, to be compliant with this requirement, the method cannot: 1) Use the same user account authenticator as the operating system, or 2) Use a decryption key that is associated with or derived from the system's local user account database or general network login credentials. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore may be appropriate for portable devices that store cardholder data.
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: ***Note:*** *This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*	**3.5** Examine key-management policies and procedures to verify processes are specified to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.	Cryptographic keys must be strongly protected because those who obtain access will be able to decrypt data. Key-encrypting keys, if used, must be at least as strong as the data-encrypting key in order to ensure proper protection of the key that encrypts the data as well as the data encrypted with that key. The requirement to protect keys from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures.

PCI DSS Requirements	Testing Procedures	Guidance
3.5.1 ***Additional requirement for service providers only:*** Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	**3.5.1** Interview responsible personnel and review documentation to verify that a document exists to describe the cryptographic architecture, including: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management	***Note:*** *This requirement applies only when the entity being assessed is a service provider.* Maintaining current documentation of the cryptographic architecture enables an entity to understand the algorithms, protocols, and cryptographic keys used to protect cardholder data, as well as the devices that generate, use and protect the keys. This allows an entity to keep pace with evolving threats to their architecture, enabling them to plan for updates as the assurance levels provided by different algorithms/key strengths changes. Maintaining such documentation also allows an entity to detect lost or missing keys or key-management devices, and identify unauthorized additions to their cryptographic architecture.
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	**3.5.2** Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.	There should be very few who have access to cryptographic keys (reducing the potential for rending cardholder data visible by unauthorized parties), usually only those who have key custodian responsibilities.

PCI DSS Requirements	Testing Procedures	Guidance
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method ***Note:*** *It is not required that public keys be stored in one of these forms.*	**3.5.3.a** Examine documented procedures to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times. • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As key components or key shares, in accordance with an industry-accepted method	Cryptographic keys must be stored securely to prevent unauthorized or unnecessary access that could result in the exposure of cardholder data. It is not intended that the key-encrypting keys be encrypted, however they are to be protected against disclosure and misuse as defined in Requirement 3.5. If key-encrypting keys are used, storing the key-encrypting keys in physically and/or logically separate locations from the data-encrypting keys reduces the risk of unauthorized access to both keys.
	3.5.3.b Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt cardholder data exist in one (or more) of the following form at all times. • Encrypted with a key-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As key components or key shares, in accordance with an industry-accepted method	
	3.5.3.c Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify: • Key-encrypting keys are at least as strong as the data-encrypting keys they protect • Key-encrypting keys are stored separately from data-encrypting keys.	
3.5.4 Store cryptographic keys in the fewest possible locations.	**3.5.4** Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations.	Storing cryptographic keys in the fewest locations helps an organization to keep track and monitor all key locations, and minimizes the potential for keys to be exposed to unauthorized parties.

PCI DSS Requirements	Testing Procedures	Guidance
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: ***Note:*** *Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*	**3.6.a** ***Additional testing procedure for service provider assessments only:*** If the service provider shares keys with their customers for transmission or storage of cardholder data, examine the documentation that the service provider provides to their customers to verify that it includes guidance on how to securely transmit, store, and update customers' keys, in accordance with Requirements 3.6.1 through 3.6.8 below.	The manner in which cryptographic keys are managed is a critical part of the continued security of the encryption solution. A good key-management process, whether it is manual or automated as part of the encryption product, is based on industry standards and addresses all key elements at 3.6.1 through 3.6.8.
	3.6.b Examine the key-management procedures and processes for keys used for encryption of cardholder data and perform the following:	Providing guidance to customers on how to securely transmit, store and update cryptographic keys can help prevent keys from being mismanaged or disclosed to unauthorized entities. This requirement applies to keys used to encrypt stored cardholder data, and any respective key-encrypting keys. ***Note:*** *Testing Procedure 3.6.a is an additional procedure that only applies if the entity being assessed is a service provider.*
3.6.1 Generation of strong cryptographic keys	**3.6.1.a** Verify that key-management procedures specify how to generate strong keys.	The encryption solution must generate strong keys, as defined in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* under "Cryptographic Key Generation." Use of strong cryptographic keys significantly increases the level of security of encrypted cardholder data.
	3.6.1.b Observe the procedures for generating keys to verify that strong keys are generated.	
3.6.2 Secure cryptographic key distribution	**3.6.2.a** Verify that key-management procedures specify how to securely distribute keys.	The encryption solution must distribute keys securely, meaning the keys are distributed only to custodians identified in 3.5.1, and are never distributed in the clear.
	3.6.2.b Observe the method for distributing keys to verify that keys are distributed securely.	
3.6.3 Secure cryptographic key storage	**3.6.3.a** Verify that key-management procedures specify how to securely store keys.	The encryption solution must store keys securely, for example, by encrypting them with a key-encrypting key. Storing keys without proper protection could provide access to attackers, resulting in the decryption and exposure of cardholder data.
	3.6.3.b Observe the method for storing keys to verify that keys are stored securely.	

PCI DSS Requirements	Testing Procedures	Guidance
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	**3.6.4.a** Verify that key-management procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s). **3.6.4.b** Interview personnel to verify that keys are changed at the end of the defined cryptoperiod(s).	A cryptoperiod is the time span during which a particular cryptographic key can be used for its defined purpose. Considerations for defining the cryptoperiod include, but are not limited to, the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted. Periodic changing of encryption keys when the keys have reached the end of their cryptoperiod is imperative to minimize the risk of someone's obtaining the encryption keys, and using them to decrypt data.
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. ***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*	**3.6.5.a** Verify that key-management procedures specify processes for the following: • The retirement or replacement of keys when the integrity of the key has been weakened • The replacement of known or suspected compromised keys. • Any keys retained after retiring or replacing are not used for encryption operations **3.6.5.b** Interview personnel to verify the following processes are implemented: • Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. • Keys are replaced if known or suspected to be compromised. • Any keys retained after retiring or replacing are not used for encryption operations.	Keys that are no longer used or needed, or keys that are known or suspected to be compromised, should be revoked and/or destroyed to ensure that the keys can no longer be used. If such keys need to be kept (for example, to support archived, encrypted data) they should be strongly protected. The encryption solution should provide for and facilitate a process to replace keys that are due for replacement or that are known to be, or suspected of being, compromised.

PCI DSS Requirements	Testing Procedures	Guidance
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. ***Note:*** *Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	**3.6.6.a** Verify that manual clear-text key-management procedures specify processes for the use of the following: • Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND • Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials (for example, passwords or keys) of another.	Split knowledge and dual control of keys are used to eliminate the possibility of one person having access to the whole key. This control is applicable for manual key-management operations, or where key management is not implemented by the encryption product. Split knowledge is a method in which two or more people separately have key components, where each person knows only their own key component, and the individual key components convey no knowledge of the original cryptographic key. Dual control requires two or more people to perform a function, and no single person can access or use the authentication materials of another.
	3.6.6 b Interview personnel and/or observe processes to verify that manual clear-text keys are managed with: • Split knowledge, AND • Dual control	
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	**3.6.7.a** Verify that key-management procedures specify processes to prevent unauthorized substitution of keys.	The encryption solution should not allow for or accept substitution of keys coming from unauthorized sources or unexpected processes.
	3.6.7.b Interview personnel and/or observe processes to verify that unauthorized substitution of keys is prevented.	
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	**3.6.8.a** Verify that key-management procedures specify processes for key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	This process will help ensure individuals that act as key custodians commit to the key-custodian role and understand and accept the responsibilities.
	3.6.8.b Observe documentation or other evidence showing that key custodians have acknowledged (in writing or electronically) that they understand and accept their key-custodian responsibilities.	
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	**3.7** Examine documentation and interview personnel to verify that security policies and operational procedures for protecting stored cardholder data are: • Documented, • In use, and • Known to all affected parties.	Personnel need to be aware of and following security policies and documented operational procedures for managing the secure storage of cardholder data on a continuous basis.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS Requirements	Testing Procedures	Guidance
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* *Examples of open, public networks include but are not limited to:* • *The Internet* • *Wireless technologies, including 802.11 and Bluetooth* • *Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* • *General Packet Radio Service (GPRS)* • *Satellite communications*	**4.1.a** Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations. **4.1.b** Review documented policies and procedures to verify processes are specified for the following: • For acceptance of only trusted keys and/or certificates • For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported) • For implementation of proper encryption strength per the encryption methodology in use **4.1.c** Select and observe a sample of inbound and outbound transmissions as they occur (for example, by observing system processes or network traffic) to verify that all cardholder data is encrypted with strong cryptography during transit. **4.1.d** Examine keys and certificates to verify that only trusted keys and/or certificates are accepted. **4.1.e** Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations. **4.1.f** Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)	Sensitive information must be encrypted during transmission over public networks, because it is easy and common for a malicious individual to intercept and/or divert data while in transit. Secure transmission of cardholder data requires using trusted keys/certificates, a secure protocol for transport, and proper encryption strength to encrypt cardholder data. Connection requests from systems that do not support the required encryption strength, and that would result in an insecure connection, should not be accepted. Note that some protocol implementations (such as SSL, SSH v1.0, and early TLS) have known vulnerabilities that an attacker can use to gain control of the affected system. Whichever security protocol is used, ensure it is configured to use only secure versions and configurations to prevent use of an insecure connection—for example, by using only trusted certificates and supporting only strong encryption (not supporting weaker, insecure protocols or methods). Verifying that certificates are trusted (for example, have not expired and are issued from a trusted source) helps ensure the integrity of the secure connection. *(Continued on next page)*

PCI DSS Requirements	Testing Procedures	Guidance
	4.1.g For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received. For example, for browser-based implementations: • "HTTPS" appears as the browser Universal Record Locator (URL) protocol, and • Cardholder data is only requested if "HTTPS" appears as part of the URL.	Generally, the web page URL should begin with "HTTPS" and/or the web browser display a padlock icon somewhere in the window of the browser. Many TLS certificate vendors also provide a highly visible verification seal—sometimes referred to as a "security seal," "secure site seal," or "secure trust seal")—which may provide the ability to click on the seal to reveal information about the website. Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.)
	4.1.h If SSL/early TLS is used, perform testing procedures in *Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.*	
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	**4.1.1** Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment. Examine documented standards and compare to system configuration settings to verify the following for all wireless networks identified: • Industry best practices are used to implement strong encryption for authentication and transmission. • Weak encryption (for example, WEP, SSL) is not used as a security control for authentication or transmission.	Malicious users use free and widely available tools to eavesdrop on wireless communications. Use of strong cryptography can help limit disclosure of sensitive information across wireless networks. Strong cryptography for authentication and transmission of cardholder data is required to prevent malicious users from gaining access to the wireless network or utilizing wireless networks to access other internal networks or data.
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	**4.2.a** If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	E-mail, instant messaging, SMS, and chat can be easily intercepted by packet-sniffing during delivery across internal and public networks. Do not utilize these messaging tools to send PAN unless they are configured to provide strong encryption.
	4.2.b Review written policies to verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies.	Additionally, if an entity requests PAN via end-user messaging technologies, the entity should provide a tool or method to protect these PANs using strong cryptography or render PANs unreadable before transmission.

PCI DSS Requirements	Testing Procedures	Guidance
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	**4.3** Examine documentation and interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are: • Documented, • In use, and • Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis.

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

PCI DSS Requirements	Testing Procedures	Guidance
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	There is a constant stream of attacks using widely published exploits, often called "zero day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. Without an anti-virus solution that is updated regularly, these new forms of malicious software can attack systems, disable a network, or lead to compromise of data.
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	**5.1.1** Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs; • Detect all known types of malicious software, • Remove all known types of malicious software, and • Protect against all known types of malicious software. *Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits.*	It is important to protect against **ALL** types and forms of malicious software.

PCI DSS Requirements	Testing Procedures	Guidance
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	**5.1.2** Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, in order to confirm whether such systems continue to not require anti-virus software.	Typically, mainframes, mid-range computers (such as AS/400) and similar systems may not currently be commonly targeted or affected by malware. However, industry trends for malicious software can change quickly, so it is important for organizations to be aware of new malware that might affect their systems—for example, by monitoring vendor security notices and anti-virus news groups to determine whether their systems might be coming under threat from new and evolving malware. Trends in malicious software should be included in the identification of new security vulnerabilities, and methods to address new trends should be incorporated into the company's configuration standards and protection mechanisms as needed
5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.	**5.2.a** Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date.	Even the best anti-virus solutions are limited in effectiveness if they are not maintained and kept current with the latest security updates, signature files, or malware protections. Audit logs provide the ability to monitor virus and malware activity and anti-malware reactions. Thus, it is imperative that anti-malware solutions be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.
	5.2.b Examine anti-virus configurations, including the master installation of the software to verify anti-virus mechanisms are: • Configured to perform automatic updates, and • Configured to perform periodic scans.	
	5.2.c Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that: • The anti-virus software and definitions are current. • Periodic scans are performed.	
	5.2.d Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that: • Anti-virus software log generation is enabled, and • Logs are retained in accordance with PCI DSS Requirement 10.7.	

PCI DSS Requirements	Testing Procedures	Guidance
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. ***Note:*** *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*	**5.3.a** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running. **5.3.b** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users. **5.3.c** Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Anti-virus that continually runs and is unable to be altered will provide persistent security against malware. Use of policy-based controls on all systems to ensure anti-malware protections cannot be altered or disabled will help prevent system weaknesses from being exploited by malicious software. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active—for example, disconnecting the unprotected system from the Internet while the anti-virus protection is disabled, and running a full scan after it is re-enabled.
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	**5.4** Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against malware are: • Documented, • In use, and • Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures to ensure systems are protected from malware on a continuous basis.

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: *Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.*

PCI DSS Requirements	Testing Procedures	Guidance
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. ***Note:*** *Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.*	**6.1.a** Examine policies and procedures to verify that processes are defined for the following: • To identify new security vulnerabilities • To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. • To use reputable outside sources for security vulnerability information. **6.1.b** Interview responsible personnel and observe processes to verify that: • New security vulnerabilities are identified. • A risk ranking is assigned to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. • Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.	The intent of this requirement is that organizations keep up to date with new vulnerabilities that may impact their environment. Sources for vulnerability information should be trustworthy and often include vendor websites, industry news groups, mailing list, or RSS feeds. Once an organization identifies a vulnerability that could affect their environment, the risk that the vulnerability poses must be evaluated and ranked. The organization must therefore have a method in place to evaluate vulnerabilities on an ongoing basis and assign risk rankings to those vulnerabilities. This is not achieved by an ASV scan or internal vulnerability scan, rather this requires a process to actively monitor industry sources for vulnerability information. Classifying the risks (for example, as "high," "medium," or "low") allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.

PCI DSS Requirements	Testing Procedures	Guidance
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. ***Note:*** *Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	**6.2.a** Examine policies and procedures related to security-patch installation to verify processes are defined for: • Installation of applicable critical vendor-supplied security patches within one month of release. • Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).	There is a constant stream of attacks using widely published exploits, often called "zero day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. If the most recent patches are not implemented on critical systems as soon as possible, a malicious individual can use these exploits to attack or disable a system, or gain access to sensitive data. Prioritizing patches for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. Consider prioritizing patch installations such that security patches for critical or at-risk systems are installed within 30 days, and other lower-risk patches are installed within 2-3 months. This requirement applies to applicable patches for all installed software, including payment applications (both those that are PA-DSS validated and those that are not).
	6.2.b For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following: • That applicable critical vendor-supplied security patches are installed within one month of release. • All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months).	
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle ***Note:*** *this applies to all software developed internally as well as bespoke or custom software developed by a third party.*	**6.3.a** Examine written software-development processes to verify that the processes are based on industry standards and/or best practices.	Without the inclusion of security during the requirements definition, design, analysis, and testing phases of software development, security vulnerabilities can be inadvertently or maliciously introduced into the production environment. Understanding how sensitive data is handled by the application—including when stored, transmitted, and when in memory—can help identify where data needs to be protected.
	6.3.b Examine written software-development processes to verify that information security is included throughout the life cycle.	
	6.3.c Examine written software-development processes to verify that software applications are developed in accordance with PCI DSS.	
	6.3.d Interview software developers to verify that written software-development processes are implemented.	

PCI DSS Requirements	Testing Procedures	Guidance
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	**6.3.1** Examine written software-development procedures and interview responsible personnel to verify that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers.	Development, test and/or custom application accounts, user IDs, and passwords should be removed from production code before the application becomes active or is released to customers, since these items may give away information about the functioning of the application. Possession of such information could facilitate compromise of the application and related cardholder data.
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release. *(Continued on next page)*	**6.3.2.a** Examine written software-development procedures and interview responsible personnel to verify that all custom application code changes must be reviewed (using either manual or automated processes) as follows: • Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release.	Security vulnerabilities in custom code are commonly exploited by malicious individuals to gain access to a network and compromise cardholder data. An individual knowledgeable and experienced in code-review techniques should be involved in the review process. Code reviews should be performed by someone other than the developer of the code to allow for an independent, objective review. Automated tools or processes may also be used in lieu of manual reviews, but keep in mind that it may be difficult or even impossible for an automated tool to identify some coding issues. Correcting coding errors before the code is deployed into a production environment or released to customers prevents the code exposing the environments to potential exploit. Faulty code is also far more difficult and expensive to address after it has been deployed or released into production environments. Including a formal review and signoff by management prior to release helps to ensure that code is approved and has been developed in accordance with policies and procedures.

PCI DSS Requirements	Testing Procedures	Guidance
Note: *This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.* *Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	**6.3.2.b** Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above.	
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	**6.4** Examine policies and procedures to verify the following are defined: • Development/test environments are separate from production environments with access control in place to enforce separation. • A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. • Production data (live PANs) are not used for testing or development. • Test data and accounts are removed before a production system becomes active. • Change control procedures related to implementing security patches and software modifications are documented.	Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced.
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	**6.4.1.a** Examine network documentation and network device configurations to verify that the development/test environments are separate from the production environment(s).	Due to the constantly changing state of development and test environments, they tend to be less secure than the production environment. Without adequate separation between environments, it may be possible for the production environment, and cardholder data, to be compromised due to less-stringent security configurations and possible vulnerabilities in a test or development environment.
	6.4.1.b Examine access controls settings to verify that access controls are in place to enforce separation between the development/test environments and the production environment(s).	

PCI DSS Requirements	Testing Procedures	Guidance
6.4.2 Separation of duties between development/test and production environments	**6.4.2** Observe processes and interview personnel assigned to development/test environments and personnel assigned to production environments to verify that separation of duties is in place between development/test environments and the production environment.	Reducing the number of personnel with access to the production environment and cardholder data minimizes risk and helps ensure that access is limited to those individuals with a business need to know. The intent of this requirement is to separate development and test functions from production functions. For example, a developer may use an administrator-level account with elevated privileges in the development environment, and have a separate account with user-level access to the production environment.
6.4.3 Production data (live PANs) are not used for testing or development	**6.4.3.a** Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Security controls are usually not as stringent in test or development environments. Use of production data provides malicious individuals with the opportunity to gain unauthorized access to production data (cardholder data).
	6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	
6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.	**6.4.4.a** Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active.	Test data and accounts should be removed before the system component becomes active (in production), since these items may give away information about the functioning of the application or system. Possession of such information could facilitate compromise of the system and related cardholder data.
	6.4.4.b Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active.	

PCI DSS Requirements	Testing Procedures	Guidance
6.4.5 Change control procedures must include the following:	**6.4.5.a** Examine documented change control procedures and verify procedures are defined for: • Documentation of impact • Documented change approval by authorized parties • Functionality testing to verify that the change does not adversely impact the security of the system • Back-out procedures	If not properly managed, the impact of system changes—such as hardware or software updates and installation of security patches—might not be fully realized and could have unintended consequences.
	6.4.5.b For a sample of system components, interview responsible personnel to determine recent changes. Trace those changes back to related change control documentation. For each change examined, perform the following:	
6.4.5.1 Documentation of impact.	**6.4.5.1** Verify that documentation of impact is included in the change control documentation for each sampled change.	The impact of the change should be documented so that all affected parties can plan appropriately for any processing changes.
6.4.5.2 Documented change approval by authorized parties.	**6.4.5.2** Verify that documented approval by authorized parties is present for each sampled change.	Approval by authorized parties indicates that the change is a legitimate and approved change sanctioned by the organization.
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	**6.4.5.3.a** For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system.	Thorough testing should be performed to verify that the security of the environment is not reduced by implementing a change. Testing should validate that all existing security controls remain in place, are replaced with equally strong controls, or are strengthened after any change to the environment.
	6.4.5.3.b For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.	
6.4.5.4 Back-out procedures.	**6.4.5.4** Verify that back-out procedures are prepared for each sampled change.	For each change, there should be documented back-out procedures in case the change fails or adversely affects the security of an application or system, to allow the system to be restored back to its previous state.

PCI DSS Requirements	Testing Procedures	Guidance
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	**6.4.6** For a sample of significant changes, examine change records, interview personnel, and observe the affected systems/networks to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change.	Having processes to analyze significant changes helps ensure that all appropriate PCI DSS controls are applied to any systems or networks added or changed within the in-scope environment. Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date and security controls are applied where needed. A change management process should include supporting evidence that PCI DSS requirements are implemented or preserved through the iterative process. Examples of PCI DSS requirements that could be impacted include, but are not limited to: • Network diagram is updated to reflect changes. • Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled. • Systems are protected with required controls—e.g., file-integrity monitoring (FIM), anti-virus, patches, audit logging. • Sensitive authentication data (SAD) is not stored and all cardholder data (CHD) storage is documented and incorporated into data-retention policy and procedures • New systems are included in the quarterly vulnerability scanning process.

PCI DSS Requirements	Testing Procedures	Guidance
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines. ***Note:*** *The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*	**6.5.a** Examine software-development policies and procedures to verify that up-to-date training in secure coding techniques is required for developers at least annually, based on industry best practices and guidance. **6.5.b** Examine records of training to verify that software developers receive up-to-date training on secure coding techniques at least annually, including how to avoid common coding vulnerabilities. **6.5.c** Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities:	The application layer is high-risk and may be targeted by both internal and external threats. Requirements 6.5.1 through 6.5.10 are the minimum controls that should be in place, and organizations should incorporate the relevant secure coding practices as applicable to the particular technology in their environment. Application developers should be properly trained to identify and resolve issues related to these (and other) common coding vulnerabilities. Having staff knowledgeable of secure coding guidelines should minimize the number of security vulnerabilities introduced through poor coding practices. Training for developers may be provided in-house or by third parties and should be applicable for technology used. As industry-accepted secure coding practices change, organizational coding practices and developer training should likewise be updated to address new threats—for example, memory scraping attacks. The vulnerabilities identified in 6.5.1 through 6.5.10 provide a minimum baseline. It is up to the organization to remain up to date with vulnerability trends and incorporate appropriate measures into their secure coding practices.

PCI DSS Requirements	Testing Procedures	Guidance
Note: *Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external).*		
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**6.5.1** Examine software-development policies and procedures and interview responsible personnel to verify that injection flaws are addressed by coding techniques that include: • Validating input to verify user data cannot modify meaning of commands and queries. • Utilizing parameterized queries.	Injection flaws, particularly SQL injection, are a commonly used method for compromising applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data, and allows the attacker to attack components inside the network through the application, to initiate attacks such as buffer overflows, or to reveal both confidential information and server application functionality. Information should be validated before being sent to the application—for example, by checking for all alpha characters, mix of alpha and numeric characters, etc.
6.5.2 Buffer overflows	**6.5.2** Examine software-development policies and procedures and interview responsible personnel to verify that buffer overflows are addressed by coding techniques that include: • Validating buffer boundaries. • Truncating input strings.	Buffer overflows occur when an application does not have appropriate bounds checking on its buffer space. This can cause the information in the buffer to be pushed out of the buffer's memory space and into executable memory space. When this occurs, the attacker has the ability to insert malicious code at the end of the buffer and then push that malicious code into executable memory space by overflowing the buffer. The malicious code is then executed and often enables the attacker remote access to the application and/or infected system.
6.5.3 Insecure cryptographic storage	**6.5.3** Examine software-development policies and procedures and interview responsible personnel to verify that insecure cryptographic storage is addressed by coding techniques that: • Prevent cryptographic flaws. • Use strong cryptographic algorithms and keys.	Applications that do not utilize strong cryptographic functions properly to store data are at increased risk of being compromised, and exposing authentication credentials and/or cardholder data. If an attacker is able to exploit weak cryptographic processes, they may be able to gain clear-text access to encrypted data.

PCI DSS Requirements	Testing Procedures	Guidance
6.5.4 Insecure communications	**6.5.4** Examine software-development policies and procedures and interview responsible personnel to verify that insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications.	Applications that fail to adequately encrypt network traffic using strong cryptography are at increased risk of being compromised and exposing cardholder data. If an attacker is able to exploit weak cryptographic processes, they may be able to gain control of an application or even gain clear-text access to encrypted data.
6.5.5 Improper error handling	**6.5.5** Examine software-development policies and procedures and interview responsible personnel to verify that improper error handling is addressed by coding techniques that do not leak information via error messages (for example, by returning generic rather than specific error details).	Applications can unintentionally leak information about their configuration or internal workings, or expose privileged information through improper error handling methods. Attackers use this weakness to steal sensitive data or compromise the system altogether. If a malicious individual can create errors that the application does not handle properly, they can gain detailed system information, create denial-of-service interruptions, cause security to fail, or crash the server. For example, the message "incorrect password provided" tells an attacker the user ID provided was accurate and that they should focus their efforts only on the password. Use more generic error messages, like "data could not be verified."
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	**6.5.6** Examine software-development policies and procedures and interview responsible personnel to verify that coding techniques address any "high risk" vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1.	All vulnerabilities identified by an organization's vulnerability risk-ranking process (defined in Requirement 6.1) to be "high risk" and that could affect the application should be identified and addressed during application development.
Note: *Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):*		Web applications, both internally and externally (public) facing, have unique security risks based upon their architecture as well as the relative ease and occurrence of compromise.
6.5.7 Cross-site scripting (XSS)	**6.5.7** Examine software-development policies and procedures and interview responsible personnel to verify that cross-site scripting (XSS) is addressed by coding techniques that include • Validating all parameters before inclusion • Utilizing context-sensitive escaping.	XSS flaws occur whenever an application takes user-supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser, which can hijack user sessions, deface web sites, possibly introduce worms, etc.

PCI DSS Requirements	Testing Procedures	Guidance
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	**6.5.8** Examine software-development policies and procedures and interview responsible personnel to verify that improper access control—such as insecure direct object references, failure to restrict URL access, and directory traversal—is addressed by coding technique that includes: • Proper authentication of users • Sanitizing input • Not exposing internal object references to users • User interfaces that do not permit access to unauthorized functions.	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization. Consistently enforce access control in presentation layer and business logic for all URLs. Frequently, the only way an application protects sensitive functionality is by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly. An attacker may be able to enumerate and navigate the directory structure of a website (directory traversal) thus gaining access to unauthorized information as well as gaining further insight into the workings of the site for later exploitation. If user interfaces permit access to unauthorized functions, this access could result in unauthorized individuals gaining access to privileged credentials or cardholder data. Only authorized users should be permitted to access direct object references to sensitive resources. Limiting access to data resources will help prevent cardholder data from being presented to unauthorized resources.
6.5.9 Cross-site request forgery (CSRF)	**6.5.9** Examine software development policies and procedures and interview responsible personnel to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers.	A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then enables the attacker to perform any state-changing operations the victim is authorized to perform (such as updating account details, making purchases, or even authenticating to the application).

PCI DSS Requirements	Testing Procedures	Guidance
6.5.10 Broken authentication and session management.	**6.5.10** Examine software development policies and procedures and interview responsible personnel to verify that broken authentication and session management are addressed via coding techniques that commonly include: • Flagging session tokens (for example cookies) as "secure" • Not exposing session IDs in the URL • Incorporating appropriate time-outs and rotation of session IDs after a successful login.	Secure authentication and session management prevents unauthorized individuals from compromising legitimate account credentials, keys, or session tokens that would otherwise enable the intruder to assume the identity of an authorized user.
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	**6.6** For *public-facing* web applications, ensure that *either* one of the following methods is in place as follows: • Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows: – At least annually – After any changes – By an organization that specializes in application security – That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment – That all vulnerabilities are corrected – That the application is re-evaluated after the corrections. • Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: – Is situated in front of public-facing web applications to detect and prevent web-based attacks. – Is actively running and up to date as applicable. – Is generating audit logs. – Is configured to either block web-based attacks, or generate an alert that is immediately investigated.	Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. The requirement for reviewing applications or installing web-application firewalls is intended to reduce the number of compromises on public-facing web applications due to poor coding or application management practices. • Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities • Web-application firewalls filter and block non-essential traffic at the application layer. Used in conjunction with a network-based firewall, a properly configured web-application firewall prevents application-layer attacks if applications are improperly coded or configured. This can be achieved through a combination of technology and process. Process-based solutions must have mechanisms that facilitate timely responses to alerts in order to meet the intent of this requirement, which is to prevent attacks. ***Note:*** *"An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.*

PCI DSS Requirements	Testing Procedures	Guidance
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	**6.7** Examine documentation and interview personnel to verify that security policies and operational procedures for developing and maintaining secure systems and applications are: • Documented, • In use, and • Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures to ensure systems and applications are securely developed and protected from vulnerabilities on a continuous basis.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS Requirements	Testing Procedures	Guidance
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	**7.1** Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows: • Defining access needs and privilege assignments for each role • Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities • Assignment of access based on individual personnel's job classification and function • Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.	The more people who have access to cardholder data, the more risk there is that a user's account will be used maliciously. Limiting access to those with a legitimate business reason for the access helps an organization prevent mishandling of cardholder data through inexperience or malice.
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.	**7.1.1** Select a sample of roles and verify access needs for each role are defined and include: • System components and data resources that each role needs to access for their job function • Identification of privilege necessary for each role to perform their job function.	In order to limit access to cardholder data to only those individuals who need such access, first it is necessary to define access needs for each role (for example, system administrator, call center personnel, store clerk), the systems/devices/data each role needs access to, and the level of privilege each role needs to effectively perform assigned tasks. Once roles and corresponding access needs are defined, individuals can be granted access accordingly.
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	**7.1.2.a** Interview personnel responsible for assigning access to verify that access to privileged user IDs is: • Assigned only to roles that specifically require such privileged access • Restricted to least privileges necessary to perform job responsibilities.	When assigning privileged IDs, it is important to assign individuals only the privileges they need to perform their job (the "least privileges"). For example, the database administrator or backup administrator should not be assigned the same privileges as the overall systems administrator. *(Continued on next page)*

PCI DSS Requirements	Testing Procedures	Guidance
	7.1.2.b Select a sample of user IDs with privileged access and interview responsible management personnel to verify that privileges assigned are: • Necessary for that individual's job function • Restricted to least privileges necessary to perform job responsibilities.	Assigning least privileges helps prevent users without sufficient knowledge about the application from incorrectly or accidentally changing application configuration or altering its security settings. Enforcing least privilege also helps to minimize the scope of damage if an unauthorized person gains access to a user ID.
7.1.3 Assign access based on individual personnel's job classification and function.	**7.1.3** Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual's job classification and function.	Once needs are defined for user roles (per PCI DSS requirement 7.1.1), it is easy to grant individuals access according to their job classification and function by using the already-created roles.
7.1.4 Require documented approval by authorized parties specifying required privileges.	**7.1.4** Select a sample of user IDs and compare with documented approvals to verify that: • Documented approval exists for the assigned privileges • The approval was by authorized parties • That specified privileges match the roles assigned to the individual.	Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:	**7.2** Examine system settings and vendor documentation to verify that an access control system(s) is implemented as follows:	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access controls systems to manage user access. ***Note:*** *Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*
7.2.1 Coverage of all system components	**7.2.1** Confirm that access control systems are in place on all system components.	
7.2.2 Assignment of privileges to individuals based on job classification and function.	**7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.	
7.2.3 Default "deny-all" setting.	**7.2.3** Confirm that the access control systems have a default "deny-all" setting.	

PCI DSS Requirements	Testing Procedures	Guidance
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	**7.3** Examine documentation and interview personnel to verify that security policies and operational procedures for restricting access to cardholder data are: • Documented, • In use, and • Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures to ensure that access is controlled and based on need-to-know and least privilege, on a continuous basis.

Requirement 8: Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

Note: *These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. This includes accounts used by vendors and other third parties (for example, for support or maintenance). These requirements do not apply to accounts used by consumers (e.g., cardholders).*

However, Requirements 8.1.1, 8.2, 8.5, 8.2.3 through 8.2.5, and 8.1.6 through 8.1.8 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).

PCI DSS Requirements	Testing Procedures	Guidance
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	**8.1.a** Review procedures and confirm they define processes for each of the items below at 8.1.1 through 8.1.8	By ensuring each user is uniquely identified—instead of using one ID for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs.
	8.1.b Verify that procedures are implemented for user identification management, by performing the following:	
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**8.1.1** Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data.	
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**8.1.2** For a sample of privileged user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval.	To ensure that user accounts granted access to systems are all valid and recognized users, strong processes must manage all changes to user IDs and other authentication credentials, including adding new ones and modifying or deleting existing ones.
8.1.3 Immediately revoke access for any terminated users.	**8.1.3.a** Select a sample of users terminated in the past six months, and review current user access lists—for both local and remote access—to verify that their IDs have been deactivated or removed from the access lists.	If an employee has left the company and still has access to the network via their user account, unnecessary or malicious access to cardholder data could occur—either by the former employee or by a malicious user who exploits the old and/or unused account. To prevent unauthorized access, user credentials and other authentication methods therefore need to be revoked promptly (as soon as possible) upon the employee's departure.
	8.1.3.b Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated.	

PCI DSS Requirements	Testing Procedures	Guidance
8.1.4 Remove/disable inactive user accounts within 90 days.	**8.1.4** Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	Accounts that are not used regularly are often targets of attack since it is less likely that any changes (such as a changed password) will be noticed. As such, these accounts may be more easily exploited and used to access cardholder data.
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.	**8.1.5.a** Interview personnel and observe processes for managing accounts used by third parties to access, support, or maintain system components to verify that accounts used for remote access are: • Disabled when not in use • Enabled only when needed by the third party, and disabled when not in use.	Allowing vendors to have 24/7 access into your network in case they need to support your systems increases the chances of unauthorized access, either from a user in the vendor's environment or from a malicious individual who finds and uses this always-available external entry point into your network. Enabling access only for the time periods needed, and disabling it as soon as it is no longer needed, helps prevent misuse of these connections. Monitoring of vendor access provides assurance that vendors are accessing only the systems necessary and only during approved time frames.
	8.1.5.b Interview personnel and observe processes to verify that third-party remote access accounts are monitored while being used.	
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**8.1.6.a** For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts.	Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access to a user's account. ***Note:*** *Testing Procedure 8.1.6.b is an additional procedure that only applies if the entity being assessed is a service provider.*
	8.1.6.b ***Additional testing procedure for service provider assessments only:*** Review internal processes and customer/user documentation, and observe implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts.	
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	**8.1.7** For a sample of system components, inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.	If an account is locked out due to someone continually trying to guess a password, controls to delay reactivation of these locked accounts stops the malicious individual from continually guessing the password (they will have to stop for a minimum of 30 minutes until the account is reactivated). Additionally, if reactivation must be requested, the admin or help desk can validate that it is the actual account owner requesting reactivation.

PCI DSS Requirements	Testing Procedures	Guidance
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**8.1.8** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.	When users walk away from an open machine with access to critical system components or cardholder data, that machine may be used by others in the user's absence, resulting in unauthorized account access and/or misuse. The re-authentication can be applied either at the system level to protect all sessions running on that machine, or at the application level.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	**8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password/phrase) for access to the cardholder data environment, perform the following: • Examine documentation describing the authentication method(s) used. • For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).	These authentication methods, when used in addition to unique IDs, help protect users' IDs from being compromised, since the one attempting the compromise needs to know both the unique ID and the password (or other authentication used). Note that a digital certificate is a valid option for "something you have" as long as it is unique for a particular user. Since one of the first steps a malicious individual will take to compromise a system is to exploit weak or nonexistent passwords, it is important to implement good processes for authentication management.

PCI DSS Requirements	Testing Procedures	Guidance
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	**8.2.1.a** Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage.	Many network devices and applications transmit unencrypted, readable passwords across the network and/or store passwords without encryption. A malicious individual can easily intercept unencrypted passwords during transmission using a "sniffer," or directly access unencrypted passwords in files where they are stored, and use this data to gain unauthorized access. ***Note:*** *Testing Procedures 8.2.1.d and 8.2.1.e are additional procedures that only apply if the entity being assessed is a service provider.*
	8.2.1.b For a sample of system components, examine password files to verify that passwords are unreadable during storage.	
	8.2.1.c For a sample of system components, examine data transmissions to verify that passwords are unreadable during transmission.	
	8.2.1.d ***Additional testing procedure for service provider assessments only:*** Observe password files to verify that non-consumer customer passwords are unreadable during storage.	
	8.2.1.e ***Additional testing procedure for service provider assessments only:*** Observe data transmissions to verify that non-consumer customer passwords are unreadable during transmission.	
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	**8.2.2** Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the authentication credential is modified.	Many malicious individuals use "social engineering"—for example, calling a help desk and acting as a legitimate user—to have a password changed so they can utilize a user ID. Consider use of a "secret question" that only the proper user can answer to help administrators identify the user prior to re-setting or modifying authentication credentials.

PCI DSS Requirements	Testing Procedures	Guidance
8.2.3 Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.	**8.2.3a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require at least the following strength/complexity: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. **8.2.3.b** ***Additional testing procedure for service provider assessments only*:** Review internal processes and customer/user documentation to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters.	Strong passwords/passphrases are the first line of defense into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords. If passwords are short or simple to guess, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID. This requirement specifies that a minimum of seven characters and both numeric and alphabetic characters should be used for passwords/ passphrases. For cases where this minimum cannot be met due to technical limitations, entities can use "equivalent strength" to evaluate their alternative. For information on variability and equivalency of password strength (also referred to as entropy) for passwords/passphrases of different formats, refer to industry standards (e.g., the current version of NIST SP 800-63.) ***Note:*** *Testing Procedure 8.2.3.b is an additional procedure that only applies if the entity being assessed is a service provider.*
8.2.4 Change user passwords/passphrases at least once every 90 days.	**8.2.4.a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require users to change passwords at least once every 90 days. **8.2.4.b** ***Additional testing procedure for service provider assessments only****: Review internal* processes and customer/user documentation to verify that: • Non-consumer customer user passwords/passphrases are required to change periodically; and • Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change.	Passwords/passphrases that are valid for a long time without a change provide malicious individuals with more time to work on breaking the password/phrase. ***Note:*** *Testing Procedure 8.2.4.b is an additional procedure that only applies if the entity being assessed is a service provider.*

PCI DSS Requirements	Testing Procedures	Guidance
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	**8.2.5.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases. **8.2.5.b** ***Additional testing procedure for service provider assessments only:*** Review internal processes and customer/user documentation to verify that new non-consumer customer user passwords/passphrase cannot be the same as the previous four passwords.	If password history isn't maintained, the effectiveness of changing passwords is reduced, as previous passwords can be reused over and over. Requiring that passwords cannot be reused for a period of time reduces the likelihood that passwords that have been guessed or brute-forced will be used in the future. ***Note:*** *Testing Procedure 8.2.5.b is an additional procedure that only applies if the entity being assessed is a service provider.*
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	**8.2.6** Examine password procedures and observe security personnel to verify that first-time passwords/passphrases for new users, and reset passwords/passphrases for existing users, are set to a unique value for each user and changed after first use.	If the same password is used for every new user, an internal user, former employee, or malicious individual may know or easily discover this password, and use it to gain access to accounts.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. ***Note:*** *Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.*		Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication (as described in Requirement 8.2), before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk. Multi-factor authentication is not required at both the system-level and application-level for a particular system component. Multi-factor authentication can be performed either upon authentication to the particular network or to the system component. Examples of multi-factor technologies include but are not limited to remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate multi-factor authentication.

PCI DSS Requirements	Testing Procedures	Guidance
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	**8.3.1.a** Examine network and/or system configurations, as applicable, to verify multi-factor authentication is required for all non-console administrative access into the CDE. **8.3.1.b** Observe a sample of administrator personnel login to the CDE and verify that at least two of the three authentication methods are used.	This requirement is intended to apply to all personnel with administrative access to the CDE. This requirement applies only to personnel with administrative access and only for non-console access to the CDE; it does not apply to application or system accounts performing automated functions. If the entity does not use segmentation to separate the CDE from the rest of their network, an administrator could use multi-factor authentication either when logging onto the CDE network or when logging onto a system. If the CDE is segmented from the rest of the entity's network, an administrator would need to use multi-factor authentication when connecting to a CDE system from a non-CDE network. Multi-factor authentication can be implemented at network level or at system/application level; it does not have to be both. If the administrator uses MFA when logging into the CDE network, they do not also need to use MFA to log into a particular system or application within the CDE.
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	**8.3.2.a** Examine system configurations for remote access servers and systems to verify multi-factor authentication is required for: • All remote access by personnel, both user and administrator, and • All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes). **8.3.2.b** Observe a sample of personnel (for example, users and administrators) connecting remotely to the network and verify that at least two of the three authentication methods are used.	This requirement is intended to apply to all personnel—including general users, administrators, and vendors (for support or maintenance) with remote access to the network—where that remote access could lead to access to the CDE. If remote access is to an entity's network that has appropriate segmentation, such that remote users cannot access or impact the cardholder data environment, multi-factor authentication for remote access to that network would not be required. However, multi-factor authentication is required for any remote access to networks with access to the cardholder data environment, and is recommended for all remote access to the entity's networks.

PCI DSS Requirements	Testing Procedures	Guidance
8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.	**8.4.a** Examine procedures and interview personnel to verify that authentication policies and procedures are distributed to all users.	Communicating password/authentication policies and procedures to all users helps those users understand and abide by the policies. For example, guidance on selecting strong passwords may include suggestions to help personnel select hard-to-guess passwords that don't contain dictionary words, and that don't contain information about the user (such as the user ID, names of family members, date of birth, etc.). Guidance for protecting authentication credentials may include not writing down passwords or saving them in insecure files, and being alert for malicious individuals who may attempt to exploit their passwords (for example, by calling an employee and asking for their password so the caller can "troubleshoot a problem"). Instructing users to change passwords if there is a chance the password is no longer secure can prevent malicious users from using a legitimate password to gain unauthorized access.
	8.4.b Review authentication policies and procedures that are distributed to users and verify they include: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials. • Instructions for users not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.	
	8.4.c Interview a sample of users to verify that they are familiar with authentication policies and procedures.	
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	**8.5.a** For a sample of system components, examine user ID lists to verify the following: • Generic user IDs are disabled or removed. • Shared user IDs for system administration activities and other critical functions do not exist. • Shared and generic user IDs are not used to administer any system components.	If multiple users share the same authentication credentials (for example, user account and password), it becomes impossible to trace system access and activities to an individual. This in turn prevents an entity from assigning accountability for, or having effective logging of, an individual's actions, since a given action could have been performed by anyone in the group that has knowledge of the authentication credentials.
	8.5.b Examine authentication policies and procedures to verify that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited.	
	8.5.c Interview system administrators to verify that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested.	

PCI DSS Requirements	Testing Procedures	Guidance
8.5.1 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. ***Note:*** *This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.*	**8.5.1** ***Additional testing procedure for service provider assessments only:*** Examine authentication policies and procedures and interview personnel to verify that different authentication credentials are used for access to each customer.	***Note:*** *This requirement applies only when the entity being assessed is a service provider.* To prevent the compromise of multiple customers through the use of a single set of credentials, vendors with remote access accounts to customer environments should use a different authentication credential for each customer. Technologies, such as multi-factor mechanisms, that provide a unique credential for each connection (for example, via a single-use password) could also meet the intent of this requirement.
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	**8.6.a** Examine authentication policies and procedures to verify that procedures for using authentication mechanisms such as physical security tokens, smart cards, and certificates are defined and include: • Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.	If user authentication mechanisms such as tokens, smart cards, and certificates can be used by multiple accounts, it may be impossible to identify the individual using the authentication mechanism. Having physical and/or logical controls (for example, a PIN, biometric data, or a password) to uniquely identify the user of the account will prevent unauthorized users from gaining access through use of a shared authentication mechanism.
	8.6.b Interview security personnel to verify authentication mechanisms are assigned to an account and not shared among multiple accounts.	
	8.6.c Examine system configuration settings and/or physical controls, as applicable, to verify that controls are implemented to ensure only the intended account can use that mechanism to gain access.	

PCI DSS Requirements	Testing Procedures	Guidance
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	**8.7.a** Review database and application configuration settings and verify that all users are authenticated prior to access.	Without user authentication for access to databases and applications, the potential for unauthorized or malicious access increases, and such access cannot be logged since the user has not been authenticated and is therefore not known to the system. Also, database access should be granted through programmatic methods only (for example, through stored procedures), rather than via direct access to the database by end users (except for DBAs, who may need direct access to the database for their administrative duties).
	8.7.b Examine database and application configuration settings to verify that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).	
	8.7.c Examine database access control settings and database application configuration settings to verify that user direct access to or queries of databases are restricted to database administrators.	
	8.7.d Examine database access control settings, database application configuration settings, and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).	
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	**8.8** Examine documentation and interview personnel to verify that security policies and operational procedures for identification and authentication are: • Documented, • In use, and • Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures for managing identification and authorization on a continuous basis.

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

PCI DSS Requirements	Testing Procedures	Guidance
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	**9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. • Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. • Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder data environment and verify that they are "locked" to prevent unauthorized use.	Without physical access controls, such as badge systems and door controls, unauthorized persons could potentially gain access to the facility to steal, disable, disrupt, or destroy critical systems and cardholder data. Locking console login screens prevents unauthorized persons from gaining access to sensitive information, altering system configurations, introducing vulnerabilities into the network, or destroying records.
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. ***Note:*** *"Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*	**9.1.1.a** Verify that either video cameras or access control mechanisms (or both) are in place to monitor the entry/exit points to sensitive areas. **9.1.1.b** Verify that either video cameras or access control mechanisms (or both) are protected from tampering or disabling.	When investigating physical breaches, these controls can help identify the individuals that physically accessed the sensitive areas, as well as when they entered and exited. Criminals attempting to gain physical access to sensitive areas will often attempt to disable or bypass the monitoring controls. To protect these controls from tampering, video cameras could be positioned so they are out of reach and/or be monitored to detect tampering. Similarly, access control mechanisms could be monitored or have physical protections installed to prevent them being damaged or disabled by malicious individuals. *(Continued on next page)*

PCI DSS Requirements	Testing Procedures	Guidance
	9.1.1.c Verify that data from video cameras and/or access control mechanisms is reviewed, and that data is stored for at least three months.	Examples of sensitive areas include corporate database server rooms, back-office rooms at retail locations that store cardholder data, and storage areas for large quantities of cardholder data. Sensitive areas should be identified by each organization to ensure the appropriate physical monitoring controls are implemented.
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. *For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.*	**9.1.2** Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly accessible network jacks.	Restricting access to network jacks (or network ports) will prevent malicious individuals from plugging into readily available network jacks and gain access into internal network resources. Whether logical or physical controls, or a combination of both, are used, they should be sufficient to prevent an individual or device that is not explicitly authorized from being able to connect to the network.
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	**9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.	Without security over access to wireless components and devices, malicious users could use an organization's unattended wireless devices to access network resources, or even connect their own devices to the wireless network to gain unauthorized access. Additionally, securing networking and communications hardware prevents malicious users from intercepting network traffic or physically connecting their own devices to wired network resources.

PCI DSS Requirements	Testing Procedures	Guidance
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	**9.2.a** Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors. • Verify procedures include the following: • Identifying onsite personnel and visitors (for example, assigning badges), • Changing access requirements, and • Revoking terminated onsite personnel and expired visitor identification (such as ID badges)	Identifying authorized visitors so they are easily distinguished from onsite personnel prevents unauthorized visitors from being granted access to areas containing cardholder data.
	9.2.b Examine identification methods (such as ID badges) and observe processes for identifying and distinguishing between onsite personnel and visitors to verify that: • Visitors are clearly identified, and • It is easy to distinguish between onsite personnel and visitors.	
	9.2.c Verify that access to the identification process (such as a badge system) is limited to authorized personnel.	
9.3 Control physical access for onsite personnel to sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	**9.3.a** For a sample of onsite personnel with physical access to sensitive areas, interview responsible personnel and observe access control lists to verify that: • Access to the sensitive area is authorized. • Access is required for the individual's job function.	Controlling physical access to sensitive areas helps ensure that only authorized personnel with a legitimate business need are granted access. When personnel leave the organization, all physical access mechanisms should be returned or disabled promptly (as soon as possible) upon their departure, to ensure personnel cannot gain physical access to sensitive areas once their employment has ended.
	9.3.b Observe personnel accessing sensitive areas to verify that all personnel are authorized before being granted access.	
	9.3.c Select a sample of recently terminated employees and review access control lists to verify the personnel do not have physical access to sensitive areas.	

PCI DSS Requirements	Testing Procedures	Guidance
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	**9.4** Verify that visitor authorization and access controls are in place as follows:	Visitor controls are important to reduce the ability of unauthorized and malicious persons to gain access to facilities (and potentially, to cardholder data). Visitor controls ensure visitors are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit. Ensuring that visitor badges are returned upon expiry or completion of the visit prevents malicious persons from using a previously authorized pass to gain physical access into the building after the visit has ended. A visitor log documenting minimum information on the visitor is easy and inexpensive to maintain and will assist in identifying physical access to a building or room, and potential access to cardholder data.
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	**9.4.1.a** Observe procedures and interview personnel to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained.	
	9.4.1.b Observe the use of visitor badges or other identification to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained.	
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	**9.4.2.a** Observe people within the facility to verify the use of visitor badges or other identification, and that visitors are easily distinguishable from onsite personnel.	
	9.4.2.b Verify that visitor badges or other identification expire.	
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	**9.4.3** Observe visitors leaving the facility to verify visitors are asked to surrender their badge or other identification upon departure or expiration.	
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	**9.4.4.a** Verify that a visitor log is in use to record physical access to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted.	
	9.4.4.b Verify that the log contains: • The visitor's name, • The firm represented, and • The onsite personnel authorizing physical access.	
	9.4.4.c Verify that the log is retained for at least three months.	

PCI DSS Requirements	Testing Procedures	Guidance
9.5 Physically secure all media.	**9.5** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).	Controls for physically securing media are intended to prevent unauthorized persons from gaining access to cardholder data on any type of media. Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone's desk.
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	**9.5.1** Verify that the storage location security is reviewed at least annually to confirm that backup media storage is secure.	If stored in a non-secured facility, backups that contain cardholder data may easily be lost, stolen, or copied for malicious intent. Periodically reviewing the storage facility enables the organization to address identified security issues in a timely manner, minimizing the potential risk.
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	**9.6** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals.	Procedures and processes help protect cardholder data on media distributed to internal and/or external users. Without such procedures data can be lost or stolen and used for fraudulent purposes.
9.6.1 Classify media so the sensitivity of the data can be determined.	**9.6.1** Verify that all media is classified so the sensitivity of the data can be determined.	It is important that media be identified such that its classification status can be easily discernible. Media not identified as confidential may not be adequately protected or may be lost or stolen. ***Note:*** *This does not mean the media needs to have a "Confidential" label attached; the intent is that the organization has identified media that contains sensitive data so it can protect it.*
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	**9.6.2.a** Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked. **9.6.2.b** Select a recent sample of several days of offsite tracking logs for all media, and verify tracking details are documented.	Media may be lost or stolen if sent via a non-trackable method such as regular postal mail. Use of secure couriers to deliver any media that contains cardholder data allows organizations to use their tracking systems to maintain inventory and location of shipments.

PCI DSS Requirements	Testing Procedures	Guidance
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	**9.6.3** Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals).	Without a firm process for ensuring that all media movements are approved before the media is removed from secure areas, the media would not be tracked or appropriately protected, and its location would be unknown, leading to lost or stolen media.
9.7 Maintain strict control over the storage and accessibility of media.	**9.7** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories.	Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time. If media is not inventoried, stolen or lost media may not be noticed for a long time or at all.
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	**9.7.1** Review media inventory logs to verify that logs are maintained and media inventories are performed at least annually.	
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	**9.8** Examine the periodic media destruction policy and verify that it covers all media and defines requirements for the following: • Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. • Storage containers used for materials that are to be destroyed must be secured. • Cardholder data on electronic media must be rendered unrecoverable (e.g., via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).	If steps are not taken to destroy information contained on hard disks, portable drives, CD/DVDs, or paper prior to disposal, malicious individuals may be able to retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as "dumpster diving," where they search through trashcans and recycle bins looking for information they can use to launch an attack. Securing storage containers used for materials that are going to be destroyed prevents sensitive information from being captured while the materials are being collected. For example, "to-be-shredded" containers could have a lock preventing access to its contents or physic ally prevent access to the inside of the container. Examples of methods for securely destroying electronic media include secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks).
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	**9.8.1.a** Interview personnel and examine procedures to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.	
	9.8.1.b Examine storage containers used for materials that contain information to be destroyed to verify that the containers are secured.	
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	**9.8.2** Verify that cardholder data on electronic media is rendered unrecoverable (e.g., via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).	

PCI DSS Requirements	Testing Procedures	Guidance
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. ***Note:*** *These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.*	**9.9** Examine documented policies and procedures to verify they include: • Maintaining a list of devices • Periodically inspecting devices to look for tampering or substitution • Training personnel to be aware of suspicious behavior and to report tampering or substitution of devices.	Criminals attempt to steal cardholder data by stealing and/or manipulating card-reading devices and terminals. For example, they will try to steal devices so they can learn how to break into them, and they often try to replace legitimate devices with fraudulent devices that send them payment card information every time a card is entered. Criminals will also try to add "skimming" components to the outside of devices, which are designed to capture payment card details before they even enter the device—for example, by attaching an additional card reader on top of the legitimate card reader so that the payment card details are captured twice: once by the criminal's component and then by the device's legitimate component. In this way, transactions may still be completed without interruption while the criminal is "skimming" the payment card information during the process. This requirement is recommended, but not required, for manual key-entry components such as computer keyboards and POS keypads. Additional best practices on skimming prevention are available on the PCI SSC website.
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.	**9.9.1.a** Examine the list of devices to verify it includes: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification. **9.9.1.b** Select a sample of devices from the list and observe devices and device locations to verify that the list is accurate and up to date. **9.9.1.c** Interview personnel to verify the list of devices is updated when devices are added, relocated, decommissioned, etc.	Keeping an up-to-date list of devices helps an organization keep track of where devices are supposed to be, and quickly identify if a device is missing or lost. The method for maintaining a list of devices may be automated (for example, a device-management system) or manual (for example, documented in electronic or paper records). For on-the-road devices, the location may include the name of the personnel to whom the device is assigned.

PCI DSS Requirements	Testing Procedures	Guidance
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). ***Note:*** *Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.*	**9.9.2.a** Examine documented procedures to verify processes are defined to include the following: • Procedures for inspecting devices • Frequency of inspections. **9.9.2.b** Interview responsible personnel and observe inspection processes to verify: • Personnel are aware of procedures for inspecting devices. • All devices are periodically inspected for evidence of tampering and substitution.	Regular inspections of devices will help organizations to more quickly detect tampering or replacement of a device, and thereby minimize the potential impact of using fraudulent devices. The type of inspection will depend on the device—for example, photographs of devices that are known to be secure can be used to compare a device's current appearance with its original appearance to see whether it has changed. Another option may be to use a secure marker pen, such as a UV light marker, to mark device surfaces and device openings so any tampering or replacement will be apparent. Criminals will often replace the outer casing of a device to hide their tampering, and these methods may help to detect such activities. Device vendors may also be able to provide security guidance and "how to" guides to help determine whether the device has been tampered with. The frequency of inspections will depend on factors such as location of device and whether the device is attended or unattended. For example, devices left in public areas without supervision by the organization's personnel may have more frequent inspections than devices that are kept in secure areas or are supervised when they are accessible to the public. The type and frequency of inspections is determined by the merchant, as defined by their annual risk-assessment process.

PCI DSS Requirements	Testing Procedures	Guidance
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	**9.9.3.a** Review training materials for personnel at point-of-sale locations to verify they include training in the following: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices • Not to install, replace, or return devices without verification • Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices) • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	Criminals will often pose as authorized maintenance personnel in order to gain access to POS devices. All third parties requesting access to devices should always be verified before being provided access—for example, by checking with management or phoning the POS maintenance company (such as the vendor or acquirer) for verification. Many criminals will try to fool personnel by dressing for the part (for example, carrying toolboxes and dressed in work wear), and could also be knowledgeable about locations of devices, so it's important personnel are trained to follow procedures at all times. Another trick criminals like to use is to send a "new" POS system with instructions for swapping it with a legitimate system and "returning" the legitimate system to a specified address. The criminals may even provide return postage as they are very keen to get their hands on these devices. Personnel always verify with their manager or supplier that the device is legitimate and came from a trusted source before installing it or using it for business.
	9.9.3.b Interview a sample of personnel at point-of-sale locations to verify they have received training and are aware of the procedures for the following: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices • Not to install, replace, or return devices without verification • Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices) • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	**9.10** Examine documentation and interview personnel to verify that security policies and operational procedures for restricting physical access to cardholder data are: • Documented, • In use, and • Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures for restricting physical access to cardholder data and CDE systems on a continuous basis.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI DSS Requirements	Testing Procedures	Guidance
10.1 Implement audit trails to link all access to system components to each individual user.	**10.1** Verify, through observation and interviewing the system administrator, that: • Audit trails are enabled and active for system components. • Access to system components is linked to individual users.	It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following:	Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up. Logging of the following events enables an organization to identify and trace potentially malicious activities
10.2.1 All individual user accesses to cardholder data	**10.2.1** Verify all individual access to cardholder data is logged.	Malicious individuals could obtain knowledge of a user account with access to systems in the CDE, or they could create a new, unauthorized account in order to access cardholder data. A record of all individual accesses to cardholder data can identify which accounts may have been compromised or misused.
10.2.2 All actions taken by any individual with root or administrative privileges	**10.2.2** Verify all actions taken by any individual with root or administrative privileges are logged.	Accounts with increased privileges, such as the "administrator" or "root" account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual.

PCI DSS Requirements	Testing Procedures	Guidance
10.2.3 Access to all audit trails	**10.2.3** Verify access to all audit trails is logged.	Malicious users often attempt to alter audit logs to hide their actions, and a record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account. Having access to logs identifying changes, additions, and deletions can help retrace steps made by unauthorized personnel.
10.2.4 Invalid logical access attempts	**10.2.4** Verify invalid logical access attempts are logged.	Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user's attempts to "brute force" or guess a password.
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	**10.2.5.a** Verify use of identification and authentication mechanisms is logged. **10.2.5.b** Verify all elevation of privileges is logged. **10.2.5.c** Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.	Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.
10.2.6 Initialization, stopping, or pausing of the audit logs	**10.2.6** Verify the following are logged: • Initialization of audit logs • Stopping or pausing of audit logs.	Turning the audit logs off (or pausing them) prior to performing illicit activities is a common practice for malicious users wishing to avoid detection. Initialization of audit logs could indicate that the log function was disabled by a user to hide their actions.
10.2.7 Creation and deletion of system-level objects	**10.2.7** Verify creation and deletion of system level objects are logged.	Malicious software, such as malware, often creates or replaces system level objects on the target system in order to control a particular function or operation on that system. By logging when system-level objects, such as database tables or stored procedures, are created or deleted, it will be easier to determine whether such modifications were authorized.

PCI DSS Requirements	Testing Procedures	Guidance
10.3 Record at least the following audit trail entries for all system components for each event:	**10.3** Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following:	By recording these details for the auditable events at 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how.
10.3.1 User identification	**10.3.1** Verify user identification is included in log entries.	
10.3.2 Type of event	**10.3.2** Verify type of event is included in log entries.	
10.3.3 Date and time	**10.3.3** Verify date and time stamp is included in log entries.	
10.3.4 Success or failure indication	**10.3.4** Verify success or failure indication is included in log entries.	
10.3.5 Origination of event	**10.3.5** Verify origination of event is included in log entries.	
10.3.6 Identity or name of affected data, system component, or resource.	**10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries.	
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*	**10.4** Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach). For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised.
10.4.1 Critical systems have the correct and consistent time.	**10.4.1.a** Examine the process for acquiring, distributing and storing the correct time within the organization to verify that: • Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time, • Systems receive time information only from designated central time server(s).	

PCI DSS Requirements	Testing Procedures	Guidance
	10.4.1.b Observe the time-related system-parameter settings for a sample of system components to verify: • Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. • Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. • Systems receive time only from designated central time server(s).	
10.4.2 Time data is protected.	**10.4.2.a** Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.	
	10.4.2.b Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	
10.4.3 Time settings are received from industry-accepted time sources.	**10.4.3** Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).	
10.5 Secure audit trails so they cannot be altered.	**10.5** Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows:	Often a malicious individual who has entered the network will attempt to edit the audit logs in order to hide their activity. Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a compromise.

PCI DSS Requirements	Testing Procedures	Guidance
10.5.1 Limit viewing of audit trails to those with a job-related need.	**10.5.1** Only individuals who have a job-related need can view audit trail files.	Adequate protection of the audit logs includes strong access control (limit access to logs based on "need to know" only), and use of physical or network segregation to make the logs harder to find and modify. Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected even if the system generating the logs becomes compromised.
10.5.2 Protect audit trail files from unauthorized modifications.	**10.5.2** Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**10.5.3** Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	**10.5.4** Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media.	By writing logs from external-facing technologies such as wireless, firewalls, DNS, and mail servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network. Logs may be written directly, or offloaded or copied from external systems, to the secure internal system or media.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	**10.5.5** Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs.	File-integrity monitoring or change-detection systems check for changes to critical files, and notify when such changes are noted. For file-integrity monitoring purposes, an entity usually monitors files that don't regularly change, but when changed indicate a possible compromise.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*	**10.6** Perform the following:	Many breaches occur over days or months before being detected. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the cardholder data environment. The log review process does not have to be manual. The use of log harvesting, parsing, and alerting tools can help facilitate the process by identifying log events that need to be reviewed.

PCI DSS Requirements	Testing Procedures	Guidance
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	**10.6.1.a** Examine security policies and procedures to verify that procedures are defined for reviewing the following at least daily, either manually or via log tools: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	Checking logs daily minimizes the amount of time and exposure of a potential breach. Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. is necessary to identify potential issues. Note that the determination of "security event" will vary for each organization and may include consideration for the type of technology, location, and function of the device. Organizations may also wish to maintain a baseline of "normal" traffic to help identify anomalous behavior.
	10.6.1.b Observe processes and interview personnel to verify that the following are reviewed at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	**10.6.2.a** Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization's policies and risk management strategy.	Logs for all other system components should also be periodically reviewed to identify indications of potential issues or attempts to gain access to sensitive systems via less-sensitive systems. The frequency of the reviews should be determined by an entity's annual risk assessment.
	10.6.2.b Examine the organization's risk-assessment documentation and interview personnel to verify that reviews are performed in accordance with organization's policies and risk management strategy.	
10.6.3 Follow up exceptions and anomalies identified during the review process.	**10.6.3.a** Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process.	If exceptions and anomalies identified during the log-review process are not investigated, the entity may be unaware of unauthorized and potentially malicious activities that are occurring within their own network.
	10.6.3.b Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed.	

PCI DSS Requirements	Testing Procedures	Guidance
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	**10.7.a** Examine security policies and procedures to verify that they define the following: • Audit log retention policies • Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online.	Retaining logs for at least a year allows for the fact that it often takes a while to notice that a compromise has occurred or is occurring, and allows investigators sufficient log history to better determine the length of time of a potential breach and potential system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach. Storing logs in off-line locations could prevent them from being readily available, resulting in longer time frames to restore log data, perform analysis, and identify impacted systems or data.
	10.7.b Interview personnel and examine audit logs to verify that audit logs are retained for at least one year.	
	10.7.c Interview personnel and observe processes to verify that at least the last three months' logs are immediately available for analysis.	
10.8 ***Additional requirement for service providers only:*** Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	**10.8.a** Examine documented policies and procedures to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	***Note:*** *This requirement applies only when the entity being assessed is a service provider.* Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the cardholder data environment. The specific types of failures may vary depending on the function of the device and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner; for example, a firewall erasing all its rules or going offline.
	10.8.b Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	

PCI DSS Requirements	Testing Procedures	Guidance
10.8.1 ***Additional requirement for service providers only*:** Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	**10.8.1.a** Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls **10.8.1.b** Examine records to verify that security control failures are documented to include: • Identification of cause(s) of the failure, including root cause • Duration (date and time start and end) of the security failure • Details of the remediation required to address the root cause	***Note:*** *This requirement applies only when the entity being assessed is a service provider.* If critical security control failures alerts are not quickly and effectively responded to, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment. Documented evidence (e.g., records within a problem management system) should support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	**10.9** Examine documentation and interview personnel to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are: • Documented, • In use, and • Known to all affected parties.	Personnel need to be aware of and following security policies and daily operational procedures for monitoring all access to network resources and cardholder data on a continuous basis.

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS Requirements	Testing Procedures	Guidance
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.*	**11.1.a** Examine policies and procedures to verify processes are defined for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis. **11.1.b** Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: • WLAN cards inserted into system components • Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.) • Wireless devices attached to a network port or network device. **11.1.c** If wireless scanning is utilized, examine output from recent wireless scans to verify that: • Authorized and unauthorized wireless access points are identified, and • The scan is performed at least quarterly for all system components and facilities. **11.1.d** If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to notify personnel.	Implementation and/or exploitation of wireless technology within a network are some of the most common paths for malicious users to gain access to the network and cardholder data. If a wireless device or network is installed without a company's knowledge, it can allow an attacker to easily and "invisibly" enter the network. Unauthorized wireless devices may be hidden within or attached to a computer or other system component, or be attached directly to a network port or network device, such as a switch or router. Any such unauthorized device could result in an unauthorized access point into the environment. Knowing which wireless devices are authorized can help administrators quickly identify non-authorized wireless devices, and responding to the identification of unauthorized wireless access points helps to proactively minimize the exposure of CDE to malicious individuals. Due to the ease with which a wireless access point can be attached to a network, the difficulty in detecting their presence, and the increased risk presented by unauthorized wireless devices, these processes must be performed even when a policy exists prohibiting the use of wireless technology. The size and complexity of a particular environment will dictate the appropriate tools and processes to be used to provide sufficient assurance that a rogue wireless access point has not been installed in the environment. *(Continued on next page)*

PCI DSS Requirements	Testing Procedures	Guidance
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	**11.1.1** Examine documented records to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points.	***For example:*** *In the case of a single standalone retail kiosk in a shopping mall, where all communication components are contained within tamper-resistant and tamper-evident casings, performing a detailed physical inspection of the kiosk itself may be sufficient to provide assurance that a rogue wireless access point has not been attached or installed. However, in an environment with multiple nodes (such as in a large retail store, call center, server room or data center), detailed physical inspection is difficult. In this case, multiple methods may be combined to meet the requirement, such as performing physical system inspections in conjunction with the results of a wireless analyzer.*
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	**11.1.2.a** Examine the organization's incident response plan (Requirement 12.10) to verify it defines and requires a response in the event that an unauthorized wireless access point is detected.	
	11.1.2.b Interview responsible personnel and/or inspect recent wireless scans and related responses to verify action is taken when unauthorized wireless access points are found.	