VT SUPERIOR COURT
WASHINGTON UNIT
CIVIL DIVISION

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT
CIVIL DIVISION

2013 SEP 5 P 12: 09

IN RE: NATURAL PROVISIONS, INC.) Docket No. 522-9-13-wncv
)

FILED

ASSURANCE OF DISCONTINUANCE

Vermont Attorney General William H. Sorrell ("the Attorney General") and Natural Provisions, Inc. ("Respondent" or "Natural Provisions") hereby agree to this Assurance of Discontinuance ("AOD") pursuant to 9 V.S.A. § 2459.

BACKGROUND

1. Respondent Natural Provisions, Inc. is a corporation incorporated under the laws of Vermont, with its principal place of business in Williston, Vermont. Natural Provisions is a health food store specializing in natural and organic products.

2. In 2012, Natural Provisions suffered a data security breach in which unknown third-parties stole credit card information belonging to Natural Provisions customers.

3. Natural Provisions became aware of the breach when informed by Det. Sgt. Bart Chamberlain of the Williston Police Department, who had been informed of the breach by one or more credit card issuers.

4. After Natural Provisions first obtained information that a security breach might have occurred at its store, it did not commence taking remedial action to resolve the security vulnerability for more than a month. It did not notify the Office of the Attorney General, comply with the Data Breach Notification Act, or

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

complete remedial action necessary to resolve the security vulnerability for more than forty-five days.

5. Prior to the security vulnerability being resolved, tens of thousands of dollars worth of credit card fraud took place, and some consumers had their credit cards compromised on more than one occasion after using them at Natural Provisions.

6. In 2012, Natural Provisions processed an average of approximately 5,500 credit card transactions per month.

7. Failure to notify consumers of a security breach for more than forty-five days is a violation of Vermont's Security Breach Notification Act, which requires, "Notice of the security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification." 9 V.S.A. § 2435(b)(1).[1]

8. Failure to notify the Attorney General of a Security Breach for more than forty-five days is a violation of the Security Breach Notification Act, which requires that the Attorney General be notified of the date of the breach, the date of discovery of the breach, and a preliminary description of the breach, within 14 days of respondent receiving notification of the breach. 9 V.S.A. § 2435(b)(3)(A)(i).[2]

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

[1] This act was amended effective May 8, 2012. The 2012 amendment introduced the 45-day time limit. Prior to the amendment notification was required "in the most expedient time possible and without unreasonable delay."

[2] This requirement went into affect with the 2012 amendment.

9. Failure to adequately protect consumers' sensitive data, which includes credit card data, constitutes an unfair act and practice under 9 V.S.A. § 2453.

10. Natural Provisions states that its failure to notify the Office of the Attorney General about the security breach, comply with the Security Breach Notice Act, or complete the remedial action necessary to resolve the security vulnerability for more than forty-five days, did not occur because of its intentional violation of or indifference about its legal obligations; it occurred because of Natural Provisions was unaware of the legal obligations that arose out of the security breach, or lacked knowledge of appropriate data security practices and procedures.

INJUNCTIVE RELIEF

Definitions

11. "Applicable Vermont Law" shall mean Chapters 62 and 63 of Title 9 of the Vermont Statutes Annotated.

12. "Cardholder Information" shall mean any electronic record of Natural Provisions containing sensitive payment card authentication data collected from the magnetic stripe of a credit or debit card in connection with a Transaction and transmitted through or stored on Natural Provisions' authorization network.

13. "Consumer" shall mean any person who has purchased merchandise from Natural Provisions and whose Personally Identifiable Information has been obtained and/or collected by Natural Provisions.

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

14. "Effective Date" shall mean the date on which Natural Provisions receives a copy of this Assurance duly executed in full by Natural Provisions and the Vermont Attorney General.

15. "Personally Identifiable Information" shall have the same meaning as defined in 9 V.S.A. §2430(5).

16. "Transaction" shall mean a retail transaction in which a Consumer has purchased merchandise from Natural Provisions.

Information Security Program

General Provisions

17. Respondent shall implement and maintain a comprehensive Information Security Program that is reasonably designed to protect the security, confidentiality, and integrity of Personally Identifiable Information, by no later than one hundred and fifty (150) days after the Effective Date of this Assurance. Such program's content and implementation shall be fully documented and shall contain administrative, technical, and physical safeguards appropriate to the size and complexity of Respondent's operations, the nature and scope of Respondent's activities, and the sensitivity of the Personally Identifiable Information, including:

    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 Personally Identifiable Information that

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

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. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (i) employee training and management; (ii) information systems, including network and software design, information processing, storage, transmission, and disposal; and (iii) prevention, detection, and response to attacks, intrusions, or other systems failures.

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 implementation and evaluation of any modification to Respondent's Information Security Program, in light of the results of the testing and monitoring of any material changes to Respondent's operations or business arrangements, or any other change in circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its Information Security Program.

Specific Provisions

18. The Attorney General and Respondent recognize that technology relating to information security is constantly changing and that current security

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

procedures, software, hardware, and other security infrastructures may become obsolete or inadequate in the future. Without either party admitting that the following provisions alone amount to reasonable actions to protect Cardholder Information or Personally Identifiable Information in the future, Respondent shall, to the extent it has not already done so:

a. Not store or otherwise maintain on its network subsequent to the authorization process the full contents of the magnetic stripe of a credit or debit card, or of any single track of such a stripe, or the CVC2/CVV2/CID[3] of any such card, or the PIN or PIN block of any such card. Respondent may retain a portion of the contents of the magnetic stripe of a credit or debit card on its network subsequent to the authorization process for a period of time for legitimate business, legal, or regulatory purpose(s), but if Respondent does so, any such Cardholder Information must be securely stored in encrypted form, be accessed by essential personnel only, and retained for no longer than necessary to achieve the business, legal, or regulatory purpose.

b. Segment appropriately from the rest of the Respondent computer system those network-based portions of the Respondent computer system that store, process, or transmit Personally Identifiable Information, including Cardholder Information, by firewalls, access controls, or other appropriate measures.

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

[3] This refers to the three- or four-digit security number printed on the back of a credit card or signature strip, called the CVC2 for MasterCard; CVV2 for Visa, and CID for Discovery or American Express.

c. Implement security password management for the portions of the Respondent computer system that store, process, or transmit Personally Identifiable Information, including Cardholder Information, including strong passwords and, with respect to Point of Sale Systems and remote access to the network, two-factor authentication.

d. Implement security patching protocol for the Respondent computer system.

e. Use Virtual Private Networks ("VPNs") or other methods at least as secure as VPNs for transmission of Personally Identifiable Information, including Cardholder Information, across open, public networks.

f. Install and maintain appropriately configured and up-to-date anti-malware software on the Respondent computer system.

g. Implement and maintain security monitoring tools, such as intrusion detection systems or other devices to track and monitor unauthorized access to the Respondent computer system. Conduct at quarterly testing and continual monitoring of the Respondent computer system.

h. Implement access control measures for the portions of Respondent's computer system that store, process, and transmit Personally Identifiable Information, including Cardholder Information. Access control measures include: (a) limiting physical and electronic access to Cardholder Information on a need-to-know basis; (b) assigning unique user IDs to persons with access to Cardholder Information; and (c)

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

generating logs or other inventories of the user accounts on the portions of Respondent's computer system used to store, process, or transmit Cardholder Information.

19. The Attorney General may audit Respondent's computer systems in a manner designed to minimize burden on respondent, no more frequently than once every six months, to be implemented by the Norwich University Center for Advanced Computing and Digital Forensics ("Norwich") for a period of three years, extended to five years should any audit reveal a security vulnerability deemed material by Norwich. Respondent shall remedy any security vulnerabilities discovered by such auditing in the most expedient time possible and without unreasonable delay, but not later than six months after notification of the issue.

Compliance with Specific Provisions

20. Compliance with Paragraphs 17(b)(ii)-(iii), 17(c), 18(b), and 18(g) shall be attained by implementation of the Trustwave TrustKeeper PCI Manager and compliance with the Payment Card Industry Data Security Standard ("PCI DSS") appropriate to Respondent. This implementation will be included in the documentation required in Paragraph 17.

21. Copies of any reports generated by Trustwave relating to Respondent's information security will be sent to the Attorney General within 10 business days.

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

22. Compliance with Paragraphs 18(a), (c), and (h) shall be attained by implementation of a Keystroke Advanced POS Version 7.10 system and compliance with the PCI DSS appropriate to Respondent. The cost of implementation of this system is acknowledged to be $15,062. This implementation will be included in the documentation required in Paragraph 17.

23. Compliance with Paragraphs 17(a), 17(b)(i), 17(d), 18(d), 18(e), and 18(f) will be attained by implementation of internal controls and procedures that will be documented in accordance. These internal controls and procedures will be included in the documentation required in Paragraph 17.

24. Implementation of Paragraphs 20-23 will satisfy the requirement for administrative, technical, and physical safeguards appropriate to the size and complexity of Respondent's operations required in Paragraph 17.

25. Within one hundred fifty (150) days following the Effective Date of this Assurance, Respondent shall identify in writing the provision(s) of paragraphs 17-18 with which it has achieved Compliance ("Compliance Certification") and/or shall submit a Compliance Plan (as defined below) with respect to any such provision(s) with which it has not achieved Compliance by that date. If Respondent has not achieved Compliance with any such provisions by that date, it shall provide written notice to the Attorney General identifying: (a) the provision(s) with which it has not yet achieved Compliance; (b) the reason(s) that Compliance has not yet been achieved or cannot be achieved; and (c) a

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

reasonable and appropriate plan and timetable for achieving Compliance with such provisions ("Compliance Plan"). After the submission by Respondent of a Compliance Plan, and until such time as Respondent submits a Compliance Certification with respect to each of the provision(s) identified in such Compliance Plan, Respondent shall submit to the Attorney General an updated Compliance Plan within the earlier of (i) thirty (30) business days after the expiration of the latest timetable specified in the most recent Compliance Plan that Respondent provided to the Attorney General (or at such later time as Respondent and the Attorney General may agree) or (ii) one hundred eighty (180) days after the date of the submission of the most recent Compliance Plan that Respondent submitted to the Attorney General (or at such later time as Respondent and the Attorney General may agree).

26. If the Attorney General disputes that any Compliance Certification or any Compliance Plan satisfies Respondent's obligations under this AOD, the Attorney General shall send Respondent a written notice of the dispute within ninety (90) days following receipt of Respondent's submission of the Compliance Certification or Compliance Plan in question.

27. If Respondent has submitted a Compliance Certification and the Attorney General has not disputed Respondent's Compliance, then the provision(s) as to which Respondent has certified Compliance in a Compliance Certification shall be fully and finally satisfied and Respondent shall have no additional obligations with respect to such provision(s); however, Respondent shall have

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

the continuing responsibility to implement and maintain a comprehensive Information Security Program that is reasonably designed to protect the security, confidentiality, and integrity of Personally Identifiable Information, as set forth therein.

Legal Compliance Program

28. Within one hundred and twenty (120) days of the Effective Date of this AOD, Respondent shall engage in a full audit of its Legal Compliance Program to ensure that it is complying with Applicable Vermont Law.

29. Respondent shall implement policies and procedures to ensure continued compliance with Applicable Vermont Law, including but not limited to procedures for notifying the Attorney General and consumers in the event of a future security breach.

30. Respondent shall report any future potential security breach to the Attorney General in the most expedient time possible, but no later than seventy-two hours after discovering that a security breach may have occurred by notification by law enforcement, a credit card processor, or a financial institution; or through Natural Provisions' internal processes or data security monitoring. The notification to the Attorney General shall include date of data breach, if known, date of discovery of potential breach, and preliminary description.

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

31. This Legal Compliance Program shall include training as appropriate of all officers, managers, and employees of Natural Provisions of their roles and responsibilities in ensuring that Natural Provisions complies with the law.

32. All officers and managers of Natural Provisions shall be provided with a copy of this Assurance of Discontinuance and be required to read the AOD as part of the Legal Compliance Program.

33. Respondent shall comply strictly with all provisions of Applicable Vermont Law.

PENALTIES

34. Natural Provisions agrees to a civil penalty of fourteen thousand, nine hundred and thirty-eight dollars ($14,938). In addition, Natural Provisions agrees to expend $15,062 to implement the Keystroke POS system, which provides security beyond that which is normally found in a business of Natural Provisions' size and industry.

35. Natural Provisions shall pay fourteen thousand, nine hundred and thirty-eight dollars ($14,938) according to the following schedule: one thousand dollars ($1,000) will be paid within ten days of the Effective Date of this AOD and by the first of each of the following two months, and two thousand dollars ($2,000) will be paid by the first of each month thereafter until the balance has been paid. Respondent 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

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

    a. Duly authorized representatives 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 relating to the subject matter of this Assurance of Discontinuance in the possession, custody, or control of Respondent, which may have counsel present.

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

OTHER TERMS

37. Natural Provisions agrees that this Assurance of Discontinuance shall be binding on Natural Provisions, its principals and officers.

38. The Attorney General hereby releases and discharges any and all claims relating to the violations of the Security Breach Notice Act and Consumer Protection Act described in this Assurance of Discontinuance.

39. This Assurance of Discontinuance, other than paragraphs 34 and 35, shall terminate on the date that all of Natural Provisions' principals convey at least 95% of their aggregate interests in the company to one or more unrelated parties as defined in 26 U.S.C. § 267.

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

40. 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 any of the parties hereto to apply to this Court at any time for orders and directions as may be necessary or appropriate to carry out or construe this Assurance of Discontinuance, to modify or terminate any of its provisions, to enforce compliance, and to punish violations of its provisions.

STIPULATED PENALTIES

41. If the Superior Court of the State of Vermont, Washington Unit enters an order finding Respondent 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 $10,000. For purposes of this Section VIII, the term "each act" shall mean: each violation of 9 V.S.A. §§ 2435, 2451-2480, or each day past any appropriate deadline in this Assurance of Discontinuance or in the Security Breach Notice Act during which Natural Provisions fails to notify the Attorney General and consumers of a future breach.

NOTICE

42. Respondent may be located at:

Natural Provisions
att: Peter Lafferty, General Manager
329 Harvest Lane, Suite 100
Williston, VT 05495

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

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

SIGNATURE PAGE FOLLOWS

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

SIGNATURE

In lieu of instituting an action or proceeding against Natural Provisions, the Office of the Attorney General, pursuant to 9 V.S.A. § 2459, accepts this Assurance of Discontinuance. By signing below, Respondent voluntarily agrees with and submits to the terms of this Assurance of Discontinuance.

DATED at St. Johnsbury, Vermont this 5th day of September, 2013.

NATURAL PROVISIONS, Inc.

By: _____
Terrence Powers, authorized agent

ACCEPTED on behalf of the Attorney General:

DATED at Montpelier, Vermont this 5th day of September, 2013.

STATE OF VERMONT
WILLIAM H. SORRELL
ATTORNEY GENERAL

By: _____
Ryan Kriger, Esq.
Assistant Attorney General
Office of Attorney General
109 State Street
Montpelier, Vermont 05609
rkriger@atg.state.vt.us
(802) 828-3170