STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

IN RE: SAMANAGE SECURITY BREACH) CIVIL DIVISION
) Docket No. 555-9-17 Wncv.
)

ASSURANCE OF DISCONTINUANCE

Vermont Attorney General Thomas J. Donovan, Jr. ("the Attorney General") and SAManage LTD. ("Respondent") hereby agree to this Assurance of Discontinuance ("AOD") pursuant to 9 V.S.A. § 2459.

REGULATORY FRAMEWORK

1. Vermont's Consumer Protection Act prohibits "[u]nfair methods of competition in commerce, and unfair or deceptive acts or practices in commerce." 9 V.S.A. § 2453.

2. Vermont's Security Breach Notice Act requires notice of security breaches to consumers and to the Attorney General, and requires contractors that maintain other businesses data to notify the business of data breaches affecting that data. 9 V.S.A. § 2435.

BACKGROUND

3. Respondent SAManage USA, Inc. ("Samanage") is a corporation incorporated under the laws of Israel and doing business as SAManage USA, Inc., incorporated under the laws of Delaware, with its principal place of business located at 117 Edinburgh South, Suite 100 Cary, NC 27511. Samanage provides business-support information technology ("IT") products and services.

4. Samanage provides a cloud-based IT support system which was used by WEX Health, Inc. ("WEX Health"), formerly Bennaissance, a contractor to the State of Vermont, for managing its IT help desk and maintenance tasks.

5. On June 2, 2016, a WEX Health employee attached a Microsoft Excel spreadsheet containing the names and social security numbers of 660 Vermonters (the "Spreadsheet") to a job ticket that was part of Samanage's cloud-based IT Support system.

6. The IT Support system communicated job tickets via a unique URL generated by a hash algorithm. Samanage did not authenticate the entity requesting information via the URL (by, for example, requesting a username and password). Anyone, anywhere, could theoretically guess the URL and type it into a standard web browser, and have access to the document.

7. In June or July 2016, a Microsoft Bing webcrawler discovered the URL and posted it to its search results. The Bing search results revealed not only the link to the spreadsheet, but previewed the contents of the spreadsheet. The search results themselves displayed the names and social security numbers of some of the Vermonters in the spreadsheet. This means that it was possible to view exposed social security numbers without clicking the link for the spreadsheet, making it impossible to know how many people actually saw the exposed data.

8. Vermont's Security Breach Notice Act defines "Personally Identifiable Information" ("PII") to include an individual's name combined with a social security number.
9 V.S.A. § 2430(5).

9. Vermont's Security Breach Notice Act defines "Security Breach" as "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).

10. The exposure of the spreadsheet including the names and social security numbers of 660 Vermonters constituted a security breach.

11. In late July 2016, a Vermonter, while searching for her own name, came across this search result. The URL contained "AWS," indicating that it was on the Amazon Web Services platform. The Vermonter contacted Amazon and the Attorney General.

12. The Attorney General contacted Amazon to try to determine how the spreadsheet got posted and to assure it was taken down.

13. On July 25, 2016, Amazon emailed an engineer at Samanage to inform Samanage that PII that it had stored on its services was publicly accessible, and asking them to remove it. The engineer did not inform the appropriate personnel at Samanage that a security breach had occurred.

14. This notification triggered Samanage's duty to immediately investigate the breach, remediate it, and notify the owner of the data, WEX Health.

15. Samanage remediated the breach by changing the Spreadsheet's security settings to require authentication.

16. However, Samanage did not:

a. immediately require authentication of documents generally; or

b. notify WEX Health that its PII had been exposed.

17. Samanage is a "Data Collector" under Vermont's Security Breach Notice Act. The act distinguishes between Data Collectors who "own or license" and those who "maintain or possess" Personally Identifiable Information ("PII"). The former have a duty to notify the Attorney General within 14 days of notice or discovery of a breach, and consumers within 45 days of notice or discovery. The latter have a duty to notify the owner or licensor of the data "of the information of any security breach immediately following discovery of the breach." 9 V.S.A. § 2435(b)(2).

18. Samanage did not notify WEX Health of the security breach until late September 2016, shortly after the Attorney General, having obtained the information from Amazon, contacted Samanage about the breach.

19. WEX Health promptly issued notice to consumers and the Attorney General, in compliance with the law.

20. Absent intervention by the Attorney General, there is no indication that Samanage planned to inform anyone of the breach.

21. Samanage's delay caused Vermont consumers to learn that their social security numbers had been exposed almost two months later than they should have.

22. Respondent admits the truth of all facts set forth in the Background section.

23. Respondent complied with the Attorney General's investigative demands and inquiries in a timely manner, and worked with the Attorney General to efficiently resolve its enforcement action.

24. The Attorney General alleges that the above conduct constitutes unfair and deceptive acts and practices under 9 V.S.A. § 2453 and violations of the Security Breach Notice Act under 9 V.S.A § 2435.

INJUNCTIVE RELIEF

Information Security Program

25. **General Provisions:** Samanage 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 sixty (60) days after the date that this Assurance is filed with the court ("Effective Date"). 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 Samanage's operations, the nature

and scope of Samanage's activities, and the sensitivity of the Personally Identifiable Information Respondent collects, 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 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 Samanage's Information Security Program, in light of the results of the testing and monitoring of any material changes to Samanage's operations or business arrangements, or any other change in circumstances that Samanage knows or has reason to know may have a material impact on the effectiveness of its Information Security Program.

26. **Specific Provisions**: Without any party admitting that the following provisions alone amount to reasonable actions to protect Personally Identifiable Information in the future, Samanage shall, to the extent it has not already done so:

a. Segment appropriately those network-based portions of the Samanage's computer system that store, process, or transmit Personally Identifiable Information by firewalls, access controls, or other appropriate measures.

b. Implement security patching protocol for Samanage's computer system.

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

d. Install and maintain appropriately configured and up-to-date anti-malware software on the Samanage's computer system.

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

f. Implement access control measures for the portions of Samanage's computer system that store, process, and transmit Personally Identifiable Information. Access control measures include: (a) limiting physical and electronic access to Personally Identifiable Information on a need-to-know basis; (b) assigning unique user IDs to persons with access to Personally Identifiable Information; and (c) generating logs or other inventories of the user accounts on the portions

of Samanage's computer system used to store, process, or transmit Personally Identifiable Information.

g. Retain logs for at least 90 days online and one additional year offline.

h. Implement user authentication for all aspects of Samanage's systems that could be exposed to public access and that could possibly store or transmit Personally Identifiable Information.

Legal Compliance Program

27. Within 120 days of both Parties signing this AOD, Samanage shall engage in a full audit of its Legal Compliance Program to ensure that it is complying with all Vermont laws, including but not limited to 9 V.S.A. Chapters 62 and 63.

28. Samanage shall implement policies and procedures to ensure continued compliance with Vermont law.

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

30. All officers and managers of Samanage 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.

31. Samanage shall comply with all provisions of Vermont law, including but not limited to provisions of 9 V.S.A. Chapters 62 and 63.

PENALTIES

32. Respondents shall pay civil penalties of Two-Hundred and Sixty-Four Thousand Dollars ($264,000) within ten days of both Parties signing this AOD. 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.

33. Respondents shall be jointly responsible for the payment of the civil penalties.

REPORTING

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

a. The Attorney General may request electronic copies of any correspondence, memoranda and other documents and records in the possession, custody, or control of Respondent that relate to the violations described in this Assurance of Discontinuance, and such documents shall be delivered to the Attorney General within 30 days or at a mutually agreed to time.

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

OTHER TERMS

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

36. The Attorney General hereby releases and discharges any and all claims arising under the Security Breach Notice Act, 9 V.S.A. §§ 2430-35, and the Consumer Protection Act, 9 V.S.A. §§ 2451-2480, that it may have against Respondents for the conduct described in the Background section between the dates of January 1, 2016 and the Effective Date.

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

38. 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

39. 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.

NOTICE

40. Respondents may be located at:

117 Edinburgh South

Suite 100

Cary, NC 27511

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

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 voluntarily agrees with and submits to the terms of this Assurance of Discontinuance.

DATED at Cary, NC, this 25 day of September, 2017.

Samanage, Ltd.

By: _____

Itay Link
Chief Financial Officer

ACCEPTED on behalf of the Attorney General:

DATED at Montpelier, Vermont this 27 day of SEPTEMBER, 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