

VT SUPERIOR COURT
WASHINGTON UNIT
MAY 22 10 14 AM '04

**STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT**

IN RE: NEW ENGLAND MUNICIPAL) CIVIL DIVISION
RESOURCE CENTER) Docket No. 288-5-19 WNCV
)
)
)

ASSURANCE OF DISCONTINUANCE

Vermont Attorney General Thomas J. Donovan, Jr. (“the Attorney General”) and New England Municipal Resource Center, LTD (“NEMRC” or “Respondent”) hereby agree to this Assurance of Discontinuance (“AOD”) pursuant to 9 V.S.A. § 2459.

REGULATORY FRAMEWORK

1. Vermont’s Consumer Protection Act (VCPA) prohibits “[u]nfair or deceptive acts or practices in commerce.” 9 V.S.A. § 2453 (a).
2. The failure of a business to maintain reasonable data security that could reasonably lead to injury to consumers, either where the business is maintaining the data of consumers or has provided a computer product which maintains consumer data, is considered an unfair act in violation of Vermont’s Consumer Protection Act.

STIPULATED FACTS

3. Respondent is a domestic corporation, registered to do business in Vermont. Respondent’s principal business address is 69 Swamp Rd, Fairfax VT.
4. Respondent provides technological products and services to all towns and cities in Vermont and entities in other states.
5. Respondent’s products and services include: municipal management software which is generally referred to as the NEMRC software (“Respondent’s software”); skill development classes and seminars; one-on-one training; consulting; and support.

6. Respondent's municipal management software program ("Respondent's software") provides module-based programs used by municipalities for specific municipal functions including grand list compilation, property tax administration, general ledger, accounts receivable, and accounts payable.

7. Respondent's software stores data required by municipalities in their day-to-day operations, including municipal employees' social security numbers and homestead property tax income sensitivity adjustments calculated pursuant to 32 V.S.A. § 6061 et seq. In addition, for any municipal employee who requests salary or wage payments via direct deposit, Respondent's software stores the bank account numbers of said employee's account, to be able to make direct deposits to the employee's account.

8. Social security and/or bank account numbers, when kept in data files containing the related individuals' first names or initials and last names, can present a cybersecurity risk of financial fraud and/or identity theft for those individuals whose data is so stored. Accordingly, Vermont defines this information as "Personally Identifiable Information (PII)" within its Security Breach Notice Act, and attaches notification obligations if it is acquired during a security breach.

9. Of the functions listed in paragraph 6 above, PII is not stored in grand lists, general ledgers and accounts receivables data files. However, PII is stored in property tax administration and accounts payable data files.

10. Respondent sells two versions of Respondent's software. The first runs locally on a municipality's computer or server. The second is a "cloud-based" version in which the municipality's software and data files are stored on a Respondent-maintained server.

11. In 2018, the Attorney General became aware of allegations that Respondent software lacked adequate data security.

12. In the course of its investigation, the Attorney General, with the assistance of a team of forensic experts from Champlain College, determined the following:

- a. With regard to Respondent's software located and stored on site at municipal offices:
- i. The Respondent's software used an algorithm to encode stored social security numbers of municipal employees and bank account numbers of municipal employees who opted to be paid via direct deposit. This same algorithm was used to encode passwords. The Attorney General's investigative team was able to decode Respondent's algorithm in an hour of focused effort.
 - ii. Assuming a bad actor were to gain physical and technological access to a server containing the Respondent's data and were able to decode Respondent's algorithm, the bad actor would be able to access PII in Respondent's property administration or accounts payable data files. Because the algorithm was used in every instance of Respondent's software, anyone who was able to decode the algorithm would be able to decode any data stored on any system. By contrast, if Respondent used more robust encryption, then even if a bad actor was able to steal a password, the actor would only be able to access the data tied to that specific password.
 - iii. The files containing data stored by the Respondent's software were stored such that they could be opened by other applications like Microsoft Excel or a text editor. This means that anyone with access to a municipality's computer network would be able to open the software files, and if that actor had decoded the algorithm, the actor would have full access to all data without having to obtain a password.
 - iv. One of Respondent's tax administration data files stored bank account numbers which were not encrypted.

v. Respondent's software gave Respondent's municipal clients control of passwords. As a result, Respondent's municipal customers were able to choose weak passwords and/or use no password at all.

b. With regard to Respondent's software on the cloud server:

- i. Any user who logged in to the cloud server was able to reach a level of privileges consistent with what would be needed to compromise every cloud user on that server. For example, the user would be able to use the command prompt to launch executable software, such as malware and keylogging software, or open a web browser to download or upload other software or files.
- ii. The cloud server lacked basic data security features like antivirus software or endpoint security, and did not log attempts to access the server from most users. These features are tools to prevent security breaches, and to determine whether a security breach has occurred and what data was exfiltrated in the event of a breach.
- iii. Once logged on as one municipality, the Attorney General's forensic experts were able to view other municipalities' database tables.

13. Upon learning of these security issues, the Attorney General contacted Respondent and, using outside data security experts worked with Respondent to implement stronger data security sufficient to diminish the immediate data security vulnerabilities.

14. NEMRC worked quickly to implement all recommendations.

15. Due to the lack of logging and other basic threat-detection measures, it would not be possible to detect many types of security breaches that may have occurred. The parties are unaware of any security breaches in the Respondent's products or in any users' data files, whether stored locally at town offices or on Respondent's cloud-based server.

16. Respondent failed to engage in the following reasonable security practices:

- a. Engaging in formal security audits.
- b. Security-focused reviews of its software code.
- c. Maintaining written data security policies.
- d. Assigning a qualified person specifically responsible for security of either Respondent's software or business practices.

17. Respondent admits the facts set forth above.

STIPULATION TO ENHANCE THE SECURITY OF RESPONDENT'S PRODUCTS

18. The Attorney General asserts that the above conduct constitutes unfair acts and practices under 9 V.S.A. § 2453.

19. This Assurance is being entered into by Respondent for the sole purpose of resolving disputed claims without the necessity for litigation, and this Assurance does not constitute an admission by Respondent of any violation of any law or regulation. However, Respondent acknowledges and admits that its cybersecurity systems required upgrading and that the Attorney General's investigation greatly assisted Respondent by identifying security weaknesses. In order to settle this matter, Respondent agrees to:

- a. Implement an Information Security Program providing stronger data security across all of Respondent's products and services, including:
 - i. Identifying material internal and external risks to the security, confidentiality, and integrity of Personally Identifiable Information kept by Respondent;
 - ii. Replacing Respondent's proprietary confidential encryption algorithm with AES256 encryption (using dynamic keys) on social security numbers, bank account numbers and password fields.
 - iii. Requiring use of stronger passwords throughout Respondent's modules;

- iv. Storing passwords using industry standard techniques;
- v. Adding additional clean up routines within the software's home folder to prevent users from leaving open files with sensitive information in them;
- vi. Enforcing strict security controls on the cloud server to prevent users from installing software or using the server in any way other than intended;
- vii. Using industry standard secure coding techniques to prevent or mitigate attacks on compiled code, including using best practices including standard code review techniques on any new code released to production;
- viii. Segmenting, as appropriate, those network-based portions of Respondent's computer system which store, process or transmit Personally Identifiable Information by firewalls, access controls, or other appropriate measures;
- ix. Implementing a security patching protocol for Respondent's computer system.
- x. Using Virtual Private Networks (VPNs) or other methods for transmission of Personally Identifiable Information across open, public networks;
- xi. Installing and maintaining appropriately configured and up-to-date anti-malware software;
- xii. Installing, maintaining, and monitoring security monitoring tools, such as intrusion detection systems or other devices to track and monitor unauthorized access;
- xiii. Establishing a log aggregation system that will ingest near real-time system, remote connection and security event logs and that retains the most recent 90 days online and one additional year offline;

- xiv. Implementing user authentication with auditing for all aspects of Respondent's systems exposed to public access that could store or transmit Personally Identifiable Information;
- b. Provide robust employee training designed to educate employees of the burgeoning risks and attendant duties inherent in Respondent's retention of personally identifiable information;
- c. Designate an employee or employees to coordinate and be accountable for Respondent's Information Security Program;
- d. Fully document Respondent's implementation of, and compliance with, Respondent's Information Security Program within sixty days of signing this Assurance;
- e. Continuously evaluate Respondent's Information Security Program via testing and monitoring designed to determine the effectiveness of the Program at protecting Personally Identifiable Information;
- f. Following such testing and/or monitoring, modify Respondent's Information Security Program as needed to protect Personally Identifiable Information.

PENALTIES, COSTS & EXPENSES

20. Respondent agrees to pay civil penalties of thirty thousand dollars (\$30,000.00) in 5 monthly installments the first of which will be made within ten days of both parties signing the AOD ("the Effective Date"). 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.

REPORTING

21. To determine or secure compliance with this AOD, on reasonable notice given to Respondent, subject to any lawful privilege, and for a three-year period from the Effective Date of this agreement:

- 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 in the possession, custody, or control of Respondent, which may have counsel present, provided that the documents and records to be inspected and copied relate to the alleged violations described in this AOD.
- b. Respondent shall submit written reports, under oath if requested, with respect to any matters contained in this AOD.

OTHER TERMS

22. Respondent agrees that this AOD shall be binding on Respondent, and its successors and assigns.

23. 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 Respondent for the conduct described in the Background section up until the Effective Date.

24. The Superior Court of the State of Vermont, Civil Division, 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 this AOD.

25. Respondent shall be subject to a tax off-set through the VT Department of Taxes if any amounts ordered are unpaid as per 32 V.S.A. § 5933.

26. 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.

27. Respondent shall not participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited by this AOD or for any other purpose that would otherwise circumvent any term of this AOD. Respondent shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this AOD.

STIPULATED PENALTIES

28. If the Superior Court of the State of Vermont, Washington Unit enters an order finding Respondent to be in violation of this AOD, then the parties agree that penalties to be assessed by the Court for violation of this AOD shall not exceed \$5,000.00 for each violation that is separate and distinct from any other violation, irrespective of the number of persons potentially affected by said violation.

NOTICE


29. Respondent's address is: 69 Swamp Rd, Fairfax VT 05454.

30. Respondent 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 Respondent, the Office of the Attorney General, pursuant to 9 V.S.A. § 2459, accepts this AOD. By signing below, Respondent voluntarily agrees with and submits to the terms of this AOD.

DATED at Montpelier, Vermont, this 20 day of May, 2019.

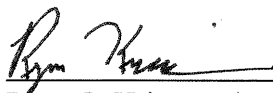
BY: 
Authorized Agent

ACCEPTED on behalf of the Attorney General:

DATED at Montpelier, Vermont this 20th day of MAY, 2019.

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

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