

STATE OF VERMONT
SUPERIOR COURT
WASHINGTON UNIT

VT SUPERIOR COURT
WASHINGTON UNIT
CIVIL DIVISION

2016 OCT 12 P 2:23

IN RE: ENTRINSIK INFORMER DATA)
SECURITY VIOLATION)

CIVIL DIVISION

Docket No. 617-10-16 Wncv

FILED

ASSURANCE OF DISCONTINUANCE

Vermont Attorney General William H. Sorrell (“the Attorney General”) and Entrinsik, Inc. (“Entrinsik” or “Respondent”) hereby agrees 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. Violations of the Vermont Consumer Protection Act are subject to a civil penalty of up to \$10,000.00 per violation. 9 V.S.A. § 2458(b)(1).

BACKGROUND

3. Respondent Entrinsik, Inc. is a corporation incorporated under the laws of the State of North Carolina, with its principal place of business located at 7721 Six Forks Road, Suite 100, Raleigh, North Carolina 27615. Entrinsik produces and sells database reporting and business intelligence software to businesses (“business consumers”), including a product currently known as Entrinsik Informer (“Informer”).

4. Seven colleges in Vermont use Informer.
5. Informer is used to analyze data and create reports by extracting data from databases and presenting it to the user. Informer operates using a web user interface, which means that the user launches a web browser, such as Microsoft’s Internet Explorer (“Internet Explorer”), and the

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

interface appears in a browser window. Informer uses functionality provided by the web browser in order to operate.

6. Informer is a horizontal web-based software product. Like other web-based software, Informer uses the web browser to display data stored on the Informer web-server, but does not use the client's computer for storing displayed information.

7. When a user who has been granted the appropriate security permissions by the business consumer exports a report containing data from Informer, Informer uses the third-party web browser's functionality to carry out the export.

8. It is not uncommon for data to be sensitive, and in some cases the use of such data may be highly regulated. For example, state law limits the use of Social Security Numbers and describes how they must be disposed of. 9 V.S.A. § 2440-45. If a business believes that such data has been lost or stolen, it has an obligation to notify the individuals whose information has been lost of the security breach. 9 V.S.A. § 2435.

9. Conscious of the legal, financial, and reputational risks associated with mishandling sensitive data, reasonable business consumers take measures to protect such data. These measures may include, among other things, requiring passwords and enforcing user roles to access such data from a database, implementing security measures such that the computers and networks housing such data cannot be accessed by those without authorization, encrypting data, and training users.

10. Informer can be expected to handle sensitive data in its regular use by business consumers.

11. Informer permits a user with the appropriate security permissions to extract sensitive data from a secure database and display the data in the browser window. It then permits such a user to export the data using various file formats, such as Excel or PDF. When a user exports such a report

he or she is prompted to name the file and choose where to store it. Thus, if the report contains sensitive information, the user has control over where the document is stored.

12. In the course of its regular and intended usage, however, the web browser in which Informer is running may, in certain instances, create and store “temporary” plain-text, unsecured files that may contain sensitive information like Social Security Numbers on a user computer’s local hard drives without the knowledge of the user or the business consumer’s Information Technology (“IT”) department.

13. Internet Explorer, for example, creates such a “temporary file” when a user selects to view a file being exported from Informer within the web browser before saving it to a selected local, secure hard drive. Internet Explorer may prompt a user to view a .csv file created with Informer by opening Excel within the browser. If this viewing option is selected by the user, Internet Explorer also generates a “temporary file” to facilitate the transaction. This is a plain-text, unencrypted, unsecured file that contains all of the potentially sensitive information. This file is given a generic file-name such as “results-184.csv” that does not indicate its sensitivity. Internet Explorer may store the file in an unsecure directory that the user may not be aware of, such as “C:\Users\\Local\AppData\Temp” (the “temp directory”). Under similar circumstances, other web browsers may store a similar “temporary file” in a download directory or elsewhere.

14. The plain-text, unsecured “temporary file” generated by the web browser when viewing certain documents within the web browser is not actually temporary. Business consumers do not generally have processes in place to clear out the temp directory, and in fact in many cases it would be a bad practice to do so because it could cause other programs that use that directory to malfunction. A reasonable business may have no knowledge that these files are being stored

locally, and if it looked for such files, it would have difficulty locating them due to their generic file-names.

15. Informer provides no warning in any of its marketing materials or user manuals that these temporary files may be created with the use of certain web browsers, which would be selected by the business consumer.

16. Any computer running Informer is at risk over time of collecting multiple plain-text files containing sensitive information. If such a computer is lost, stolen, or hacked, such information runs the risk of falling into the hands of unauthorized individuals. Such unauthorized acquisition of sensitive Personally Identifiable Information, as defined in 9 V.S.A. § 2430(5), may trigger a business's duty under Vermont law to notify consumers of a Security Breach as defined in 9 V.S.A. § 2430(8)(A).

17. An Informer user at a Vermont college generated a report that contained 14,000 Social Security Numbers and stored the report securely. However, the web browser used by the college with Informer (in this case, Internet Explorer) also stored a text file containing the 14,000 social security numbers on the computer's local hard drive, which was then backed up by the college to an external drive. In June 2013, this hard drive was misplaced, triggering the college's duty to notify the 14,000 Social Security Number owners as required by the Security Breach Notice Act. Had the web browser running with Informer not placed a "temporary" text file on the hard drive, there would have been no Security Breach.

18. Entrinsik admits the truth of all facts set forth in the Background section.

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

20. Entrinsik denies that it violated Vermont Law.

21. The parties agree that this AOD is entered into for settlement purposes only and does not constitute an admission of the violation of any law, rule, or regulation by Respondent.

INJUNCTIVE RELIEF

22. Entrinsik will take the following actions:

Within 30 days of entry of this Assurance of Discontinuance, Entrinsik will:

- i. Add clear and conspicuous warnings in all of its user and instructional materials for Informer of the functionality that creates the plain-text files described in the Background section above (a copy of the warnings to be included in these materials going forward is attached as **Exhibit 1** hereto); and
- ii. Add functionality to Informer, including any future applications that provide the same functionality of Informer, such that in the export dialog, the user will see the following message: "**Note: Exporting data may result in the creation of unsecure/unencrypted temporary or permanent files on your computer. Please contact your system administrator with any questions regarding the proper safeguarding of sensitive information.**" The message will be obviously placed (at the top of the dialog) and colored differently to make it stand out. The inclusion of this warning in the export dialog will be the default setting for Informer, and the warning will appear each time a user exports data. The user's system administrator may alter the default configuration so that this warning is deleted if the administrator so desires, but that will be a special

configuration setting, require access to the installation files in the system, and will require a restart to implement.

- iii. Issue a patch or other software update to all business consumers in Vermont that use Informer that includes the new warning and strongly recommend that the patch/software update containing the new functionality be applied. (A copy of the correspondence to be sent to all business consumers in Vermont who use Informer is attached as **Exhibit 2** hereto.)

REPORTING

23. Within forty-five (45) days of entry of this entry of this Assurance of Discontinuance, Respondent shall confirm in writing to the Attorney General, c/o Ryan Kriger, Assistant Attorney General, Office of the Attorney General, 109 State Street, Montpelier, Vermont 05609, that the actions required in paragraph 22 have been completed. Within thirty (30) days of receipt of Respondent's written confirmation, the Attorney General may request a demonstration of the Informer export function and/or the user and instructional materials described above from Respondent.

OTHER TERMS

24. Entrinsik agrees that this Assurance of Discontinuance shall be binding on Entrinsik, and its successors and assigns.

25. This AOD constitutes a complete settlement with, and general release of, Entrinsik by the Attorney General of all claims, causes of action, damages, restitution, fines, costs, attorneys' fees, penalties, and other remedies, monetary, injunctive or otherwise, that the Attorney General could have asserted or obtained under applicable law, state or federal, including but not limited to the

Vermont Consumer Protection Act, 9 V.S.A. §§ 2451-2480, 9 V.S.A. §§ 2430-2445, and Vermont common law, relating to or arising from the conduct that is the subject of this AOD against Entrinsik and its current or former parents, subsidiaries, predecessors, successors, assigns and affiliates of any kind, as well as the owners, officers, directors, employees, agents, attorneys, and heirs thereof.

26. The Superior Court of the State of Vermont, Washington Unit, shall have jurisdiction over this AOD and the parties hereto for the limited purpose of enabling any of the parties to apply to this Court at any time for orders and directions as may be necessary or appropriate to carry out or construe this AOD, to modify or terminate any of its provisions, and to enforce compliance with, or to punish violations of, this AOD. Entrinsik does not otherwise waive any defense it may have to the jurisdiction of Vermont state courts.

27. 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

28. If the Superior Court of the State of Vermont, Washington Unit, enters an order finding Respondent to be in violation of the injunctive relief agreed to by the parties in this Assurance of Discontinuance, then the parties agree that penalties to be assessed by the Court for each act in violation of this AOD shall be \$5,000. For purposes of this Section, the term "each act" shall mean: failure to comply with any individual element of the injunctive relief (i.e., subparagraphs (i) – (iii) of paragraph 22 above) required under this AOD with regard to each customer of Entrinsik in Vermont.

NOTICE

29. Respondent may be located at:

Entrinsik, Inc.
c/o Mr. Douglas Leupen
7721 Six Forks Road, Suite 100
Raleigh, North Carolina 27615
DLeupen@entrinsik.com
(919) 848-4828

With copy to:

Morningstar Law Group
W. Swain Wood
swood@morningstarlawgroup.com
J. Christopher Jackson
cjackson@morningstarlawgroup.com
(919) 829-7394

30. Respondent shall notify the Attorney General of any change of business name or address within 30 business days of the change.

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

SIGNATURE

In lieu of instituting an action or proceeding against Entrinsik, 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 RALEIGH, NC, this 5th day of SEI OCT, 2016.

ENTRINSIK, INC.

By: 
Its Authorized Agent
Douglas Leupen, CEO

ACCEPTED on behalf of the Attorney General:

DATED at Montpelier, Vermont this 4th day of OCTOBER, 2016.

STATE OF VERMONT

WILLIAM H. SORRELL
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

EXHIBIT 1

A warning about Exporting Data from Informer

Informer uses a web browser to deliver data to the user. If a user's security settings within Informer allow them to export data, then they can download the results of a report, archive, or dashboard to variety of formats, onto their computer or device. Exporting data may result in the creation of insecure and/or unencrypted temporary or permanent files on your computer.

The location of the downloaded file is a configurable computer setting outside the scope of Informer. The downloaded file may be saved to a well-known directory, such as the "Downloads" directory. Or it may instead be saved to another, potentially unsecure directory that the user may not be aware of, such as "C:\Users\\Local\AppData\Temp." This happens even if the user chooses "Open" at the time of export.

These files are unencrypted, and except for PDF format, are plain text files. The user or system administrator should be fully aware that this is happening before granting permission for Informer users to export data.

It should be noted that this behavior cannot be controlled by Informer, apart from forbidding exporting completely. Users should contact their system administrator with any questions regarding the proper safeguarding of sensitive information that may be downloaded from Informer.

EXHIBIT 2

Entrinsik is proud to announce the release of Informer 4.7. This release contains huge speed and capacity improvements for dashboards.

You are strongly urged to upgrade to this release, as it contains an important warning about exporting data. When users attempt to export data they will now see this warning:

Note: Exporting data may result in the creation of unsecure/unencrypted temporary or permanent files on your computer. Please contact your system administrator with any questions regarding the proper safeguarding of sensitive information.

The full release notes are here: <https://entrinsikinraleigh.zendesk.com/hc/en-us/articles/202367485-Release-Notes>

Please note: If you have dashboards, this upgrade involves installing new software, so please allow for more time.

To upgrade your current system to version 4.7, visit the [Informer customer portal](#), select "Installation/upgrades," then "Download Informer Upgrades" under the "Upgrades" heading.

Documentation and release notes on Informer 4.7 can be found in the customer portal under "[Documentation](#)."

Have questions about upgrading your system? Email support@entrinsik.com or call 1-888-703-0016.