

RECEIVED

DEC 02 2019

CONSUMER PROTECTION

November 26, 2019

**David H. Potter**  
312.821.6106 (direct)  
David.Potter@wilsonelser.com

**Via Postal Mail Only**

**Attorney General Gordon J. MacDonald**  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent the Ivy Rehab Network (“Ivy Rehab”), headquartered in White Plains, New York, with respect to a potential data security incident described in more detail below. Ivy Rehab takes the security and privacy of the information in its control very seriously and has implemented remedial and proactive measures to prevent a similar incident from occurring in the future.

**1. Nature of the security incident.**

Ivy Rehab is an outpatient rehabilitation provider offering physical therapy, occupational therapy, and speech language pathology services. In May of 2019, while investigating a fraudulent invoice that was processed, Ivy Rehab found evidence to suggest that a limited number of Ivy Rehab employee email accounts may have been inappropriately accessed. Ivy Rehab then immediately conducted an internal investigation with the assistance of its internal and external IT team and found additional evidence that certain email accounts may have been accessed by unknown unauthorized parties. Subsequently, Ivy Rehab changed the affected employees’ email credentials.

Ivy Rehab then engaged Wilson Elser and, through Wilson Elser, an independent computer forensic company to determine the nature and extent of the unauthorized access. Ivy Rehab determined that the incident affected the email accounts belonging to nine (9) Ivy Rehab employees in various positions and locations throughout the company. Ivy Rehab, with the assistance of an additional service provider engaged through counsel, then conducted a search of the affected email accounts to determine if any personal information and/or protected health information was accessible to the unknown unauthorized parties. The investigation concluded on September 26, 2019 and revealed that the accessed email accounts may have contained patient

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky  
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix • San Diego  
San Francisco • Sarasota • Stamford • Virginia • Washington, DC • West Palm Beach • White Plains

**wilsonelser.com**

information including patients' names in combination with one or more of the following: protected health information, Social Security number, and/or financial account information. However, as of this writing, Ivy Rehab has no evidence that patients' personal or protected health information was misused as a consequence of this incident.

**2. Number of New Hampshire residents affected.**

A total of eleven (11) New Hampshire residents may have been potentially affected by this incident. Notification letters to these individuals were mailed on November 26, 2019, by first class mail. A sample copy of the notification letter is included with this letter.

**3. Steps taken.**

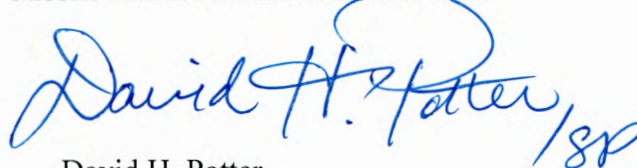
Ivy Rehab takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar event from occurring in the future, as well as to protect the privacy and security of potentially impacted individuals' information. This includes, but is not limited to, forcing password changes for all employees' email accounts, two-factor authentication, enhancing endpoint security systems, and re-educating employees about how to identify and prevent malicious emails and phishing campaigns. Notice was provided to the U.S. Department of Health and Human Services Office of Civil Rights on November 26, 2019. Ivy Rehab is also providing potentially impacted individuals with identify theft protection and credit monitoring services for a period of twelve (12) months, at its own expense, through Equifax.

**4. Contact information.**

Ivy Rehab remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at [David.Potter@wilsonelser.com](mailto:David.Potter@wilsonelser.com) or (312) 821-6106.

Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**



David H. Potter

Enclosure.

1311 Mamroneck Avenue, Suite 140  
White Plains, New York 10605



7-7-1-FPDBR420112519130615 LETTER1

Not CA,CT,MA,NY,RI Adult  
186 GARLAND ST  
SPRINGFIELD, ND, 01118-2219

November 25, 2019

Dear Not CA,CT,MA,NY,RI Adult:

We are writing to inform you of an incident involving the Ivy Rehab Network of providers ("Ivy Rehab") that may have resulted in unauthorized access to some of your personal information, including your health information. While we have no indication that your information has been misused, we are nonetheless providing you with notice of this incident out of an abundance of caution. We take the privacy and protection of your personal information very seriously. Your trust is a top priority at Ivy Rehab, and we deeply regret any inconvenience this may cause you. This letter contains information about what happened, steps we have taken to mitigate the risk of harm, and complimentary resources we are making available to protect you.

In May of 2019, we found evidence to suggest that a limited number of Ivy Rehab employee email accounts may have been accessed by unknown unauthorized parties. We then immediately conducted an internal investigation with the assistance of our internal and external IT team and found additional evidence to suggest that certain email accounts may have been accessed by unknown unauthorized parties. Subsequently, we engaged a leading computer forensic firm to investigate the nature and extent of the unauthorized access to our email system. The investigation identified certain employee email accounts that were potentially accessed by unauthorized parties as a result of a presumed phishing campaign targeting our employees.

On September 26, 2019, after a search of the contents of the affected email accounts, we discovered that the accessed email accounts may have contained patient information including one or more of the following: your health information, Social Security number, and/or financial account information. Once again, we have no evidence of misuse of anyone's information as a consequence of this incident. Nonetheless, we are notifying you of this incident out of an abundance of caution.

In light of this incident, we are offering complimentary services to protect you for a period of twelve months. We have secured the services of Equifax to provide you with identity monitoring services. Information about the services being provided by Equifax is included with this letter.

We take data privacy and security very seriously and are actively taking steps to guard against something like this from happening again. Such steps include, but are not limited to, requiring frequent password changes, providing all staff with ongoing security awareness training, and working with government agencies where applicable. We will continue to invest resources to improve our data protection capabilities.

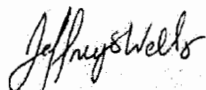


(Continued)

00000007 00013 00001-00002

We sincerely regret any inconvenience that this matter may cause you and remain dedicated to protecting your information. Please see the addendum for additional steps you can take to protect your personal information. If you have any questions, please call 833-935-1376, Monday through Friday, 9:00 a.m. to 9:00 p.m., Eastern Time.

Sincerely,

A handwritten signature in cursive script that reads "Jeffrey Wells".

Jeffrey Wells, Esq., CHC, OHCC  
Chief Compliance Officer and Privacy Officer  
Ivy Rehab Physical Therapy

**For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina:** It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

**For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:** It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

**For residents of Iowa:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

**For residents of Oregon:** State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

**For residents of Maryland, Rhode Island, Illinois, New York and North Carolina:** You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**Maryland Office of the Attorney General** Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

**Rhode Island Office of the Attorney General** Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400  
[www.riag.ri.gov](http://www.riag.ri.gov)

**North Carolina Office of the Attorney General** Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001  
1-877-566-7226 [www.ncdoj.com](http://www.ncdoj.com)

**Federal Trade Commission** Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT  
(438-4338) [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**New York Office of Attorney General** Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755  
<https://ag.ny.gov/consumer-frauds/identity-theft>

**For residents of Massachusetts:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

**For residents of Massachusetts:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

**For residents of all states:**

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud\\_Alert\\_Request\\_Form.pdf](https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf)); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

**Monitoring:** You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

**Security Freeze:** You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

**Equifax Security Freeze**

P.O. Box 105788  
Atlanta, GA 30348  
[www.freeze.equifax.com](http://www.freeze.equifax.com)  
800-525-6285

**Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013  
[www.experian.com/freeze](http://www.experian.com/freeze)  
888-397-3742

**TransUnion (FVAD)**

P.O. Box 2000  
Chester, PA 19022  
[freeze.transunion.com](http://freeze.transunion.com)  
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

00000007 00013 00002-00002





Enter your Activation Code: 459267860986

## Product Information

### Equifax® Credit Watch™ Gold with WebDetect Features

- Equifax® credit file monitoring and alerts to key changes to your Equifax credit report
- Wireless alerts (available online only) Data charges may apply.
- Access to your Equifax credit report
- Internet Scanning<sup>1</sup> Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.
- Automatic Fraud Alerts<sup>2</sup> with a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit
- Up to \$25,000 Identity Theft Insurance<sup>3</sup>
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

## Enrollment Instructions

To sign up online for online delivery go to [http://myservices.equifax.com/efx1\\_bresngis](http://myservices.equifax.com/efx1_bresngis)

- 1. Welcome Page:** Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.
- 2. Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.
- 3. Create Account:** Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.
- 4. Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.
- 5. Order Confirmation:** This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

## Identity Restoration

If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity. To be eligible for Identity Restoration, you must complete the enrollment process for the subscription offer by the enrollment deadline above. Call the phone number listed in your online member center for assistance.

<sup>1</sup>Internet scanning, will scan for your Social Security number (if you choose to), up to 5 bank account numbers, up to 6 credit/debit card numbers you provide, up to 3 email addresses, up to 10 medical ID numbers, and up to 5 passport numbers. Internet scanning scans thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and is constantly adding new sites to those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that Internet scanning is able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

<sup>2</sup>The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

<sup>3</sup> Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.