

Melissa K. Ventrone
312 580 2219 direct
mventrone@thompsoncoburn.com

July 31, 2017

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Dear Attorney General Foster:

We represent Northwest Rheumatology (“NW Rheumatology”) with respect to a recent security incident involving the potential exposure of certain protected health information described in more detail below. NW Rheumatology is a rheumatology clinic in Tucson, Arizona.

1. Nature of security incident.

On April 10, 2017, Northwest Rheumatology experienced a ransomware incident which left a limited portion of its computer system encrypted and inaccessible. NW Rheumatology immediately contacted its computer security vendor who investigated the matter and informed NW Rheumatology that no protected health information was accessed or acquired during the incident. Based on this report, NW Rheumatology believed that the attack on its systems was limited and that patient information was not affected.

However, on June 18, 2017, NW Rheumatology discovered additional evidence of unauthorized access to its systems from the ransomware attack. NW Rheumatology immediately hired an independent computer forensic firm to conduct an in-depth investigation. On July 6, 2017, the forensic team confirmed that an unauthorized individual had gained access to NW Rheumatology systems but was unable to determine whether any protected health information had actually been accessed.

2. Number of New Hampshire residents affected.

NW Rheumatology has identified records for two (2) New Hampshire residents impacted as a result of this incident. A notification letter was mailed to the individuals on July 31, 2017 via regular mail. Enclosed please find a copy of the notification letter.

3. Steps you have taken or plan to take relating to the incident.

NW Rheumatology is taking steps to prevent this sort of incident from occurring in the future. NW Rheumatology has reviewed and updated its internal password policies with new, more rigorous requirements, and has implemented new security measures to further secure the information in its systems from unauthorized access..

RECEIVED

AUG 04 2017

CONSUMER PROTECTION

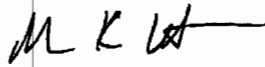
July 31, 2017
Page 2

4. Contact information.

NW Rheumatology remains dedicated to protecting the sensitive information in its systems. If you have any questions or need additional information, please do not hesitate to contact me at MVentrone@ThompsonCoburn.com or (312) 580-2219.

Very truly yours,

Thompson Coburn LLP

A handwritten signature in black ink, appearing to read "M K Ventrone", with a long horizontal flourish extending to the right.

Melissa K. Ventrone

Enclosures

NORTHWEST RHEUMATOLOGY

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name1>>

<<Address1>>

<<Address2>>

<<City>>, <<ST>> <<ZIP>>

<<Country>>

<<Date>>

Notice of Data Security Incident

Dear <<Name1>>:

We are writing to inform you about a data security incident experienced by Northwest Rheumatology ("NW Rheumatology") that may have exposed your personal information, including your name and Social Security number. We value and respect the privacy of your information, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

1. What happened and what information was involved?

On April 10, 2017, NW Rheumatology experienced a ransomware attack that encrypted a limited amount of information on our systems. We immediately had our computer security vendor conduct an investigation. The vendor informed us that no personal health data was accessed or acquired by an unauthorized individual. Based on this report, we believed our systems, and the information stored in our systems, were secure.

On June 18, 2017, while finalizing our internal recovery efforts related to the incident, our computer security vendor informed us that they had discovered additional evidence of unauthorized access to our systems. We immediately hired an independent computer forensic firm to conduct an in-depth investigation. On July 6, 2017, our forensic investigator informed us that an unauthorized individual had gained access to our systems, but they could not tell us whether any personal health information was accessed as a result of this access.

Because we are unable to determine with certainty that your information was not accessed, we thought it important to inform you of this incident and provide you with resources to help you protect your information. From our review, it appears that your name, address, Social Security number, health insurance information, diagnosis information, medical records, diagnoses, and demographic data may have been stored on our systems.

2. What we are doing and what you can do.

Securing your personal information is important to us. As a precautionary measure to help better protect your credit file from potential misuse, we have partnered with Equifax[®] to provide its Credit Watch[™] Silver credit monitoring and identity theft protection product for one year at no charge to you. A description of this product is provided below, along with instructions about how to enroll (including your personal activation code).

If you choose to take advantage of this product, it will provide you with a notification of key changes to your Equifax credit file, up to \$25,000 Identity Theft Insurance¹ Coverage, automatic fraud alerts², access to your Equifax credit report and 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.

Even if you decide not to take advantage of the subscription offer, you may still receive Equifax Identity Restoration in the event that you become victim of identity theft by calling 877-368-4940, 9:00a.m. to 8:00p.m. Eastern, Monday through Friday, before July 31, 2018.

You must complete the enrollment process for Equifax Credit Watch[™] Silver by October 31, 2017. We urge you to consider enrolling in this product, at our expense, and reviewing the Additional Resources enclosed with this letter.



Activation Code: <<INSERT Credit Monitoring Code>>

About the Equifax Credit Watch™ Silver identity theft protection product

Equifax Credit Watch will provide you with an “early warning system” to changes to your credit file and help you to understand the content of your Equifax credit file. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- Comprehensive credit file monitoring of your Equifax credit report with daily notification of key changes to your credit file.
- Wireless alerts and customizable alerts available
- One copy of your Equifax Credit Report™
- \$25,000 in identity theft insurance with \$0 deductible, at no additional cost to you †
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality *
- 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.

How to Enroll: You can sign up online

To sign up online for **online delivery** go to www.myservices.equifax.com/silver

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.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf

Please review the enclosed additional information section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

We want to assure you that we are taking steps to prevent this sort of incident from occurring in the future. NW Rheumatology has reviewed and updated its internal password policies with new, more rigorous requirements, and we have rolled out new security measures to further secure the information in our systems from unauthorized access.

3. For more information.

If you have questions, please call 800-342-9326 Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time. Please have your membership number ready. Your trust is a top priority for us, and we deeply regret any inconvenience or concern this matter may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Ulker Tok". The signature is stylized with a large initial "U" and a long horizontal stroke.

Dr. Ulker Tok
NW Rheumatology

U.S. State Notification Requirements

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 by contacting any one or more of the following national consumer reporting agencies:

Equifax

P.O. Box 105139
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 6790
Fullerton, CA 92834
1-800-916-8800
www.transunion.com

You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) 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, as well as the Federal Trade Commission.

For residents of Maryland, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys 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

**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

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft

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 at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three credit bureaus is below:

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 send a request to each consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. You may obtain a 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.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
<http://www.experian.com/freeze>

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
www.transunion.com

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