WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

February 23, 2021

Anjali C. Das
821.618.6164 (direct)
Anjali.Das@WilsonElser.com

NOTICE OF CYBERSECURITY INCIDENT

Attorney General Wayne Stenehjem
Office of Attorney General
600 East Boulevard Avenue, Department 125
Bismarck, ND 58505-0040

Via Email – NDAG@nd.gov

Dear Attorney General Stenehjem,

We represent the Jacobson Memorial Hospital & Care Center ("Jacobson Memorial" or "JMHCC"), a healthcare provider based in Elgin, North Dakota. This notice is in regard to a data incident that occurred at Jacobson Memorial. Jacobson Memorial takes the security and privacy of the information in its control seriously, and took steps to mitigate the effects of the incident that occurred.

Description of the Nature & Circumstance of the Breach

As noted above, Jacobson Memorial is a health care provider located in Elgin, North Dakota. Jacobson Memorial has been servicing the Elgin area since 1977. Unfortunately, on or about July 28, a Jacobson Memorial employee's business email account was compromised by a bad actor, and used to send out spam. Jacobson Memorial immediately conducted an internal investigation with the help of its IT vendor, and had ejected the threat actor by August 5, creating a window of compromise of approximately one week.

Jacobson Memorial proceeded to engage a separate specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the compromise. The forensics investigation was concluded on August 25, 2020, and confirmed that the compromise was limited to a single email account. Thereafter, Jacobson Memorial hired a third party vendor to conduct an automated data mining exercise to identify emails within the compromised account that contained personal information ("PII") and/or personal health information ("PHI"). This exercise was completed on September 27, 2020. Finally, Jacobson Memorial worked with the vendor to complete a manual review of the emails containing PII and PHI to identify the affected population. We received the results of the manual review on December 31, 2020.

At this time, we have no reason to believe that any individual's information has been misused. Furthermore, while we have not been able to identify the threat actor as of yet, based on their actions within the email account, the threat actor's primary motivation appears to have been to send out spam. However, in the interest of complete transparency, the inbox contained information about individuals including their name, address, date of birth, email address, social security number, phone number, insurance policy number, credit

card number, bank account number, and some patient records containing health information. The data elements at issue varied by individual; not every individual had every data field compromised. To reiterate, we have no reason to believe that anyone's information has been misused as a result of this incident.

Residents Affected

Based on our information, we believe that approximately 1,544 individuals may have been affected as a result of this incident.

Remediation

Jacobson Memorial is committed to ensuring the security of all personal information in our control. We have taken steps to mitigate the risk of future issues by completing a review of our policies, implemented enhanced security measures, and added a new facility-wide security system. Furthermore, Jacobson Memorial has implemented new policies to better protect data in its control and has already begun further training its staff and vendors on data protection.

Although we have no reason to believe that anyone's data is being misused, as an added precaution, we are working with Equifax to provide consumers with complimentary identity monitoring services.

Jacobson Memorial notified the affected individuals on February 23, provided notice to the three major consumer credit monitoring bureaus, and has set up a call center to provide constituents with information about the incident. A sample variable text version of the letter is enclosed with this letter. Finally, Jacobson Memorial purchased credit and dark web monitoring services for all affected individuals.

Contact Information

Jacobson Memorial 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 Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>,

Out of an abundance of caution, we are writing to inform you of a data security incident that involved Jacobson Memorial Hospital & Care Center ("Jacobson Memorial"). The cybersecurity incident may have resulted in the potential compromise of some of your data. Jacobson Memorial takes the security of your information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident and steps you can take to protect your information.

What Happened

Jacobson Memorial has been servicing the Elgin area since 1977. Unfortunately, on or about August 5, 2020, Jacobson Memorial learned that one of their employee's email account was compromised by a bad actor, and used to send out spam. Jacobson Memorial immediately conducted an internal investigation with the help of its IT vendor. The investigation showed that the threat actor was able to access the inbox as early as July 28, 2020, creating a window of compromise of approximately one week.

Jacobson Memorial proceeded to engage a separate specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the compromise. The forensics investigation was concluded on August 25, 2020, and confirmed that the compromise was limited to a single email account. Thereafter, Jacobson Memorial hired a third party vendor to conduct an automated data mining exercise to identify emails within the compromised account that contained personal information ("PII") and/or personal health information ("PHI"). This exercise was completed on September 27, 2020. Finally, Jacobson Memorial worked with the vendor to complete a manual review of the emails containing PII and PHI to identify the affected population. We received the results of the manual review on December 31, 2020.

What Information Was Involved

Based on the investigation and review of the compromised account, the inbox contained information about individuals including their name, address, date of birth, email address, social security number, phone number, insurance policy number, credit card number, bank account number, and some patient records containing health information. Note that the data elements varied by individual; not every individual had every element exposed. While we have no reason to believe that your information has been misused as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency.

What We Are Doing

Jacobson Memorial is committed to ensuring the security of all personal information in our control. We have taken steps to mitigate the risk of future issues by completing a review of our policies, implemented enhanced security measures, and added a new facility-wide security system. However, as always, we recommend that you continue to join us in remaining vigilant to protect your information.

We have also engaged Equifax to provide you with complimentary credit monitoring and identity theft services for a period of twelve (12) months. We encourage you to register for these complimentary services. Information about the services being provided, registration information, along with additional information about how to protect yourself, is included in the materials attached to this letter.

What You Can Do

We recommend that you continue to remain vigilant in monitoring your personal information. The easiest way to do this is to take advantage of the complimentary credit monitoring and identity theft services we are offering to you. Details regarding these services are included in a separate attachment to this letter.

There are additional steps you can take to protect yourself which are contained in the supplement to this letter titled "*Additional Important Information*."

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause your family. If you have any questions, please do not hesitate to call 844-746-4682 during the hours of 8:00 a.m. and 8:00 p.m. Central Time, Monday through Friday.

Sincerely,

Theo Stoller, MSB, LNHA
CEO/Administrator
Jacobson Memorial Hospital Care Center
601 East Street North, Elgin, North Dakota 58533

Additional Important Information

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, 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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 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

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580 1-877-IDTHEFT (438-4338) 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 all states:

Fair Credit Reporting Act: You are also advised that you may have additional rights under the federal Fair Credit Reporting Act.

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); 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	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
(800)-525-6285	(888)-397-3742	(800)-680-7289
https://www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze	freeze.transunion.com

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

EQUIFAX®

Activation Code: <<Activation Code>>

About the Equifax Credit Watch™ Gold with WebDetect identity theft protection product	Equifax Credit Watch provides you with the following key features and benefits:
Equifax Credit Watch Gold with WebDetect will provide you with an "early warning system" to changes to your credit file. Note: You must be over age 18 with a credit file in order to take advantage of the product.	○ Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax** credit report ○ Wireless alerts and customizable alerts available (available online only) ○ Access to your Equifax Credit Report™ ○ Ability to receive alerts if your Social Security Number or credit card numbers are found on Internet trading sites via WebDetect [1] ○ Up to $25,000 in identity theft insurance with $0 deductible, at no additional cost to you † ○ Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m. to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance, and help initiate an investigation of inaccurate information. ○ 90 day Fraud Alert placement with automatic renewal functionality* (available online only)

How to Enroll: To sign up online for **online delivery** go to: www.myservices.equifax.com/goldscan

1. Welcome Page: Enter the Activation Code provided at the top of this page 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.

1. WebDetect will scan for your Social Security number (if you choose to) and up to 10 major credit/debit card numbers you provide. WebDetect 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 WebDetect is able to locate and search every possible internet site where consumers' personal information is at risk of being traded.

† Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. 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. This product is not intended for minors (under 18 years of age).

* The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.