BakerHostetler

Baker&Hostetler LLP

1735 Market Street
Suite 3300
Philadelphia, PA 19103-7501

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

March 29, 2024

VIA EMAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Formella:

We are writing on behalf of our client, Rehabilitation Hospital of Southern New Mexico ("Facility"), regarding a data security incident.

On February 1, 2024, Facility was alerted to unusual activity in its Information Technology ("IT") environment. In response, Facility promptly secured and isolated its IT systems. Facility also commenced an investigation with assistance from a third-party cybersecurity firm and has been in communication with law enforcement.

Through Facility's ongoing investigation, it determined that an unauthorized party gained access to its IT network between the dates of January 16, 2024 and February 4, 2024. While in Facility's IT network, the unauthorized party accessed and/or acquired files that contain information pertaining to certain Facility patients including

On March 29, 2024, Facility mailed a notification letter to one New Hampshire resident via U.S. First-Class Mail in accordance with the Health Insurance Portability and Accountability Act (45 CFR § 160.404) and N.H. Rev. Stat. Ann. § 359-C:20. A sample copy of the notification letter is enclosed.[1] Facility is providing individuals whose
may have been involved complimentary memberships to credit monitoring and identity theft

[1] This report does not waive Facility's objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.

protection services. Facility also established a dedicated, toll-free incident response line individuals can call with questions about the incident.

To help prevent something like this from happening again, Facility has implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor its systems.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Sara M. Goldstein
Partner

Enclosure

<<Var Data 1 – Facility Name>>
Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

<<Name1>>
<<Name2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

Dear << Name1>>:

<<Var Data 1 – Facility Name>> is committed to protecting the confidentiality and security of the information we maintain. We are writing to let you know about a data security incident that may have involved some of your information. This letter explains the incident, measures that have been taken, and some steps you can take in response to protect your information.

On February 1, 2024, we were alerted to unusual activity in our Information Technology ("IT") environment. In response, we promptly secured and isolated our IT systems. We also commenced an investigation with assistance from a third-party cybersecurity firm and have been in communication with law enforcement.

Through our ongoing investigation, we determined that an unauthorized party gained access to our IT network between the dates of January 16, 2024 and February 4, 2024. While in our IT network, the unauthorized party accessed and/or acquired files that contain information pertaining to certain patients. Our investigation cannot rule out the possibility that, as a result of this incident, files containing some of your information may have been subject to unauthorized access. This information may have included your name and one or more of the following: <<Data Elements>>.

As a precaution, we are offering you a complimentary r membership to Identity Defense Complete, which includes credit monitoring and fraud alerts. **For more information on identity theft prevention and Identity Defense Complete, including instructions on how to activate your complimentary membership, please see the pages following this letter.**

We deeply regret any inconvenience or concern this incident may cause and take this matter seriously. To help prevent something like this from happening again, we have implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor our systems. If you have any questions about this incident, please call 1-844-563-2187, Monday through Friday, between 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

Identity Defense

Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>
Service Term: << CM Length>> *

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit {{URL}}

1. Enter your unique Activation Code <<Activation Code>>
   Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
   Enter your email address, create your password, and click 'Create Account'.
3. Register
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at .

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.
**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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

<<Var Data 1 – Facility Name>>'s mailing address is <<Variable Data 2 – Facility Address>> and its phone number is <<Var Data 3 – Facility Phone>>.

Additional information for residents of the following states:

Maryland Residents: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.marylandattorneygeneral.gov

New York Residents: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina Residents: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island Residents: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia Residents: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.