BakerHostetler

Baker&Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Eric A. Packel
direct dial: 215.564.3031
epackel@bakerlaw.com

September 4, 2020

VIA EMAIL (ATTORNEYGENERAL@DOJ.NH.GOV)

Attorney General Gordon MacDonald
New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Freeport Regional Healthcare Foundation ("FHN"), to notify you of a security incident involving one New Hampshire resident. FHN is a covered entity under the Health Insurance Portability & Accountability Act ("HIPAA").[1]

FHN's ongoing investigation into an email compromise incident recently determined that a limited number of FHN employees' email accounts may have been accessed by an unauthorized person. At that time, it was not known specifically what information may have been contained in the accounts. After identifying suspicious activity within the employees' email accounts, FHN immediately took steps to secure the accounts and a leading computer forensic firm was engaged to assist with the investigation. The investigation determined that an unauthorized person accessed the accounts between February 12, 2020 and February 13, 2020. The investigation was unable to determine whether the unauthorized person actually viewed any emails or attachments in the accounts. Out of an abundance of caution, FHN reviewed all of the emails and attachments contained in the email accounts to identify patient information that may have been accessible to the unauthorized person. Through this review, FHN has identified the name, date of birth, Social Security number, health insurance information, and limited treatment and/or clinical information of one New Hampshire resident.

On September 4, 2020, FHN will mail a notification letter to the New Hampshire resident

[1] This notice does not waive FHN's objection that New Hampshire lacks jurisdiction over it regarding any claims related to this incident.

pursuant to HIPAA (45 CFR §§ 160.103 and 164.400 *et seq.*) and N.H. Rev. Stat. § 359-C:20(c),[2] in substantially the same form as the enclosed letter. FHN is offering eligible individuals a complimentary one-year membership to credit monitoring and identity theft protection services. FHN has also established a dedicated, toll-free call center where all individuals may obtain more information regarding the incident.

To help prevent something like this from happening in the future, FHN reinforced education with staff regarding how to identify and avoid suspicious emails and is making additional security enhancements to its email environment, including enabling multi-factor authentication.

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

Sincerely,

Eric A. Packel
Partner

Enclosure

[2] Please note that an additional four New Hampshire residents were notified pursuant to HIPAA, but the information contained in the accounts for these individuals does not constitute Personal Information as defined by N.H. Rev. Stat. § 359-C:19(IV).

FHN
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

[redacted]

A-10494

September 4, 2020

Dear [redacted]:

FHN takes the privacy and security of its patients' information very seriously. Regrettably, we are writing to inform you that we recently identified and addressed a security incident that may have involved some of your information. This notice explains the incident, outlines the measures we have taken in response, and steps you can take.

On April 30, 2020, our ongoing investigation into an email compromise incident determined that a limited number of FHN employees' email accounts may have been accessed by an unauthorized person. At that time, it was not known specifically what information may have been contained in the accounts. After identifying suspicious activity within the employees' email accounts, we immediately took steps to secure the accounts and a leading computer forensic firm was engaged to assist with our investigation. The investigation determined that an unauthorized person accessed the accounts between February 12, 2020 and February 13, 2020. The investigation was unable to determine whether the unauthorized person actually viewed any emails or attachments in the accounts. Out of an abundance of caution, we reviewed all of the emails and attachments contained in the email accounts to identify patient information that may have been accessible to the unauthorized person. As a result of that review, we identified one or more emails and/or attachments that may have included your name, date of birth, Social Security number, medical record or patient account number, health insurance information, and limited treatment and/or clinical information, such as provider name, diagnosis, or medication information.

There is no evidence that any of your information was actually viewed by the unauthorized person, or that it has been misused. However, we wanted to notify you of this incident and assure you we take this very seriously. As a precaution, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides identity protection services focused on identification and resolution of identity theft. IdentityWorks℠ Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks℠ Credit 3B, including instructions on how to activate the complimentary one-year membership, please see the additional information provided with this letter. We also recommend that you review statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, please contact your insurer or provider immediately.

We deeply regret any concern or inconvenience this incident may cause you. To help prevent something like this from happening in the future, we reinforced education with our staff regarding how to identify and avoid suspicious emails and are making additional security enhancements to our email environment, including enabling multi-factor authentication. If you have any questions, please call us at 1-888-800-3306, Monday through Friday, between 8:00 a.m. and 5:00 p.m. Central Time.

Sincerely,

Tammy Pals
FHN Privacy Officer

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **November 16, 2020** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-288-8057** by **November 16, 2020**. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877-288-8057**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). 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 and Credit or Security Freezes:

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.

Additional information for residents of the following states:

Maryland: FHN is located at 1045 W Stephenson Street, Freeport, IL 61032, and can be reached at 877-600-0346. 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.oag.state.md.us

New York: 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; *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: 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: 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

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.