BakerHostetler

Baker&Hostetler LLP

One North Wacker Drive
Suite 4500
Chicago, IL 60606-2841

T 312.416.6200
F 312.416.6201
www.bakerlaw.com

Aleksandra M. Vold
direct dial: 312.416.6249
avold@bakerlaw.com

March 12, 2020

VIA OVERNIGHT MAIL

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Notice of Security Incident

Dear Attorney General Foster:

On December 19, 2019, on behalf of our client, Outreach Health Services ("Outreach Health"), we notified your office of a security incident involving unauthorized access to an employee email account that included information related to two New Hampshire residents.[1] In that notice, we explained that Outreach Health provided notification via United States First-Class mail to the New Hampshire residents on December 19, 2019.

Subsequently, on October 18, 2019, through additional investigation, Outreach Health discovered unauthorized access to a limited number of additional employee email accounts. Outreach Health immediately began an internal investigation, and a leading computer forensic firm was hired to assist. The investigation determined that an unauthorized person gained access to an employee email accounts between August 19 and October 13, 2019. 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, Outreach Health reviewed the emails and attachments in the accounts to identify individuals whose information may have been accessible to the unauthorized person. From this review, on December 13, 2019, Outreach Health determined that the accounts may have contained the name, address, date of birth, Social Security number and/or driver's license number, tax identification number, passport number,

[1] This notice does not waive Outreach Health's objection that New Hampshire lacks personal jurisdiction over the company related to this matter.

financial account information, health insurance information and clinical information, which may have included diagnosis, prescription, and/or treatment information of one additional New Hampshire resident.

On March 12, 2020, pursuant to HIPAA, 45 CFR §§ 160.103 and 164.400 *et seq.*, Outreach Health mailed a letter to the New Hampshire resident, via United States First-Class mail, in substantially the same form as the enclosed letter. Outreach Health is providing a toll-free telephone number for individuals to call with any questions about the incident, and it is offering individuals whose Social Security numbers and/or driver's license number were contained in the email account with one year of complimentary credit monitoring and identity theft protection services through Experian's® IdentityWorks℠. This notification is being provided in compliance with NH Rev. Stat. §359-C:20. To date, Outreach Health has notified a total of three New Hampshire residents.

To help prevent something like this from happening in the future, Outreach Health is reinforcing employee training on detecting and avoiding phishing emails and is instituting additional security measures.

Outreach Health is committed to protecting personal information. Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Aleksandra M. Vold
Counsel

Enclosures

outreach
HEALTH

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Outreach Health Services ("Outreach Health") understands the importance of safeguarding your personal information. Regrettably, we are writing to inform you of an incident that involves some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On October 18, 2019, as part of an ongoing investigation, we discovered unauthorized access to a limited number of employee email accounts. We immediately began an internal investigation, and a leading computer forensic firm was hired to assist. The investigation determined that an unauthorized person gained access to the employee email accounts between August 19, 2019 and October 13, 2019. 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 the emails and attachments in the accounts to identify individuals whose information may have been accessible to the unauthorized person. From this review, on December 13, 2019, we determined that the accounts may have contained your name, address, date of birth, Social Security number and/or driver's license number, health insurance information, and clinical information, which may have included your diagnosis, prescription, and/or treatment information. If you previously provided your tax identification number, passport number, and/or financial account information to Outreach Health, that information may also have been contained in the accounts.

While we have no indication that your information was actually viewed by the unauthorized person, or that it has been misused, we wanted to notify you of this incident and assure you that we take it very seriously. Out of an abundance of caution, 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 you with identity protection services focused on immediate 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 your complimentary one-year membership, as well as information on additional steps you can take in response, please see the additional information provided in this letter.

We deeply regret any inconvenience or concern this incident may cause you. We continually evaluate and modify our practices to enhance the security and privacy of your personal information. To help prevent something like this from happening in the future, we are reinforcing employee training on detecting and avoiding phishing emails and are instituting additional security measures.

If you have any questions, please call 1-855-946-0124, Monday through Friday, between 8:00a.m. and 5:30p.m. Central Time.

Sincerely,

John David Ball
Chief Executive Officer
Outreach Health Services
251 Renner Parkway
Richardson, Texas 75080

ELN-????-????

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **<<b2b_text_1 (Date)>>** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code: <<Member ID>>**

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. Be prepared to provide engagement number **<<b2b_text_2 (Engagement #)>>** 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.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* 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

If you are a resident of Maryland, New York, or North Carolina, 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
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov
- *New York Attorney General's Office*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov; New York Department of State, One Commerce Plaza, 99 Washington Ave, Albany, NY 12231-0001, (518) 474-8583, www.dos.ny.gov; New York State Police, 1220 Washington Avenue, Building 22, Albany, NY 12226-2252, (212) 459-7800, troopers.ny.gov

[FOR RESIDENTS OF WV—CAN DELETE IF NO WV RECIPIENTS]: **If you are a resident of West Virginia**, 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 below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of 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 (1) 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

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

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

[FOR RESIDENTS OF NM—CAN DELETE IF NO NM RECIPIENTS]: **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). Here is a summary of your major rights under FCRA. 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.