BakerHostetler

Baker&Hostetler LLP

Washington Square, Suite 1100
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5403

T 202.861.1500
F 202.861.1783
www.bakerlaw.com

Aaron R. Lancaster
direct dial: 202.8961.1501
alancaster@bakerlaw.com

June 11, 2018

Via Overnight Mail

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol St
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Health Management Concepts, Inc. ("HMC"), to notify you of a security incident involving New Hampshire residents.

On January 25, 2018, HMC learned that a computer belonging to one of its employees was infected with ransomware. The files that were encrypted as a result of the ransomware included files that contained personnel information. When HMC learned about the incident, it immediately secured the employee's computer, restored relevant files from backup, took steps to prevent any remote access to HMC's systems, began an investigation and engaged a leading forensic firm. HMC conducted a thorough investigation of the ransomware incident and determined on April 30, 2018 that some of the files that may have been accessible to the attackers included files that contained some personal information, which may have included New Hampshire residents' names and Social Security numbers.

Today, HMC will begin notifying four New Hampshire residents via U.S. mail in accordance with N.H. Rev. Stat. Ann. § 359-C:20 in substantially the same form as the enclosed letter.[1] HMC is offering eligible individuals one year of complimentary credit monitoring and identity protection services. HMC also has established a call center that potentially affected individuals can contact with questions and is recommending that potentially affected individuals remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity.

[1] This report does not waive HMC's objection that New Hampshire lacks personal jurisdiction regarding HMC.

To help prevent something like this from happening in the future, HMC conducted an extensive audit of its systems and related system access from outside entities to determine if its security measures require additional enhancement. HMC is implementing the recommendations from that audit, including providing additional monitoring of attempts to enter its systems through firewalls, open DNS ports, and emails; adding multi-factor authentication on key administrative accounts; and providing additional staff training.

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

Sincerely,

Aaron R. Lancaster
Counsel

Enclosure

HMC HealthWorks
Smarter Healthcare Decisions™

C/O GCG
P.O. Box 10646
Dublin, Ohio 43017-9246

June 11, 2018

<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

Dear <<Name1>>:

Health Management Concepts, Inc. ("HMC") values its relationship with its employees, former employees, and their families and understands the importance of protecting their personal information. We are writing to inform you that we recently identified and addressed a security incident that may have involved that personal information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On January 25, 2018, we learned that a computer belonging to one of our employees was infected with ransomware. The files that were encrypted as a result of the ransomware include files that contained personnel information. When we learned about the incident, we immediately secured the employee's computer, restored relevant files from backup, took steps to prevent any remote access to HMC's systems, began an investigation, and engaged a leading forensic firm. We conducted a thorough investigation of the ransomware incident and determined on April 30, 2018 that some of the files that may have been accessible to the attackers included files that contained your name and Social Security number.

At this time, we have no evidence that any of your information was actually accessed in any way. Nevertheless, we are notifying you of this incident out of an abundance of caution. As a precaution, we also are offering a complimentary one-year membership in 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, please see the additional information provided in this letter. We recommend that you regularly review your account statements for unauthorized activity.

We sincerely regret that this incident occurred and apologize for any inconvenience or concern this may cause you. To help prevent something like this from happening in the future, we have conducted an extensive audit of our systems and related system access from outside entities to determine if our security measures require additional enhancement. We are implementing the recommendations from that audit, including providing additional monitoring of attempts to enter our systems through firewalls, open DNS ports, and emails; adding multi-factor authentication on key administrative accounts; and additional staff training. If you have any questions or want clarification on what information may have been accessible, please call (877) 884-3610, Monday through Friday between 9 a.m. and 9 p.m. Eastern Time.

Sincerely,

Bart Bracken
Chief Operating Officer and Chief Privacy Officer

Activate IdentityWorks Credit 3B Now in Three Easy Steps

- Ensure that you **enroll by**: **09/30/2018** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/3bcredit**
- Provide your **activation code**: **[code]**

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 877.890.9332 by **09/30/2018.** Be prepared to provide engagement number **DB07236** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 877.890.9332. 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.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

Regardless of whether you choose to take advantage of this free credit monitoring, we recommend that you remain 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 Connecticut or Maryland you may contact and obtain information from your state attorney general at:

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us,
1-888-743-0023 (toll free when calling within Maryland)
(410) 576-6300 (for calls originating outside Maryland)

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 at least 90 days. 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 may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three (3) major reporting agencies by regular, certified, or overnight mail at the addresses below:

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

In order 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 (5) 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 three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) 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, you must call or send a written request to the credit reporting agencies by mail 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 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail 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 three (3) business days after receiving your request to remove the security freeze.