McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

November 24, 2020

VIA U.S. MAIL

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

Re: Aspire Health Alliance – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Aspire Health Alliance ("Aspire"). I am writing to provide notification of an incident at Blackbaud, Aspire's third-party software and service provider, that may affect the security of personal information of approximately two (2) New Hampshire residents. Aspire's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Aspire does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On September 9, 2020, Blackbaud notified Aspire of a security incident that impacted its clients across the world. Blackbaud reported to Aspire that they identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed Aspire that they stopped the ransomware attack and engaged forensic experts to assist in their internal investigation. That investigation concluded that the threat actor intermittently removed data from Blackbaud's systems between February 7, 2020 and May 20, 2020.

Once Aspire was informed of the issue, Aspire immediately initiated an internal investigation. As a part of its investigation, in addition to demanding detailed information from Blackbaud about the nature and scope of the incident, Aspire engaged outside experts experienced in handling these types of incidents to help determine the impact to its stakeholders and appropriately notify them. On October 26, 2020, Aspire determined that the information removed by the threat actor may have contained a limited amount of personal information, including full names, checking account numbers, and the banks where those accounts are held. Social Security numbers and health information were not exposed as a result of this incident.

According to Blackbaud, they paid the threat actor to ensure that the data was permanently destroyed, and there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Blackbaud also indicates that it has hired a third-party team of experts, including a team of forensics accountants, to continue monitoring for any such activity. Nevertheless, out of an abundance of caution, Aspire wanted to inform you

(and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Aspire is providing the affected residents with written notification of this incident commencing on or about November 25, 2020, in substantially the same form as the letter attached hereto. Aspire is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are being advised to contact their financial institutions to inquire about steps to take to protect their accounts. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Aspire, protecting the privacy of personal information is a top priority. Aspire remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Blackbaud has assured Aspire that they closed the vulnerability that allowed the incident and that they are enhancing their security controls and conducting ongoing efforts against incidents like this in the future. Aspire continually evaluates and modifies its practices, and those of its third party service providers, to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

Dominic A. Paluzzi

Encl.

Aspire Health Alliance
[redacted]

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear [redacted]

The privacy and security of the personal information we maintain is of the utmost importance to Aspire Health Alliance ("Aspire"). We are writing with important information regarding a recent data security incident at Blackbaud, a third party service provider, which may have involved some of the information that you provided to Aspire. Blackbaud is a software and service provider that is widely used for accounting and donor engagement efforts at non-profits and health organizations world-wide. Aspire uses a Blackbaud application and Blackbaud recently experienced an incident impacting that application. We want to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

On September 9, 2020 Blackbaud notified Aspire of a security incident that impacted its clients across the world. Blackbaud reported to us that they identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed us that they stopped the ransomware attack and engaged forensic experts to assist in their internal investigation. That investigation concluded that the threat actor intermittently removed data from Blackbaud's systems between February 7, 2020 and May 20, 2020. According to Blackbaud, they paid the threat actor to ensure that the data was permanently destroyed.

What We Are Doing.

Once we were informed of the issue, we immediately initiated an internal investigation. As a part of our investigation, in addition to demanding detailed information from Blackbaud about the nature and scope of the incident, we engaged outside experts experienced in handling these types of incidents to help determine the impact to our stakeholders and appropriately notify them.

What Information Was Involved.

On October 26, 2020 we determined that the information removed by the threat actor may have contained some of your personal information, including your full name and checking account number and the bank where that account is held. **Your Social Security number and health information was not exposed as a result of this incident.**

What You Can Do.

According to Blackbaud, there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Blackbaud indicates that it has hired a third-party team of experts, including a team of forensics accountants, to continuing monitoring for any such activity. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

This letter provides precautionary measures that you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis and report any suspicious activity to the proper authorities. Because your bank or financial account number was impacted, you may want to contact your financial institution to discuss ways in which you can best protect your account, including possibly changing your account number or flagging your account.

For More Information.

We sincerely regret any inconvenience this incident may cause you. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. Blackbaud has assured us that they closed the vulnerability that allowed the incident and that they are enhancing their security controls and conducting ongoing efforts against incidents like this in the future. We continually evaluate and modify our practices, and those of our third party service providers, to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call us directly at [redacted], Monday through Friday, 9 a.m. to 5 p.m. We can share information on the incident and direct you to resources to help you protect your information.

Sincerely,

Aspire Health Alliance

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

You may place an initial one (1) year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

2. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-349-9960

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.