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

November 30, 2020

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
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, Maimonides Medical Center ("MMC"), regarding an incident that occurred at one of its vendors, Blackbaud, Inc. ("Blackbaud").

Blackbaud is a third-party vendor that provides customer relationship management and financial services tools for fundraising purposes to thousands of schools, non-profits and health systems, including MMC. Blackbaud notified many of its customers, including MMC, that it discovered a data security incident involving the Blackbaud systems. Blackbaud further advised that the unauthorized access occurred between February 7, 2020 and May 20, 2020 and that the unauthorized actors acquired backup copies of databases used by its customers, including a backup of the database that stores some of MMC's information. Once MMC was notified, MMC immediately took steps to understand the extent of the incident and the data involved, which included reviewing the specific contents of the database to determine what it contained.

On September 25, 2020, based on MMC's investigation and review of the Blackbaud database involved in the incident, MMC determined that it contained general demographic information and images of checks used to make donations, which include bank account numbers and routing numbers for three (3) New Hampshire residents.

Importantly, MMC does not store Social Security numbers in the Blackbaud database. This incident did not involve any access to MMC's medical systems or electronic health records. Additionally, if individuals previously made donations by credit card, Blackbaud informed MMC

that any credit card information in the database was encrypted, and therefore not able to be accessed by the unauthorized individual.

MMC mailed notification letters to the New Hampshire residents on November 30, 2020 in accordance with N.H. Rev. Stat. Ann. § 359-C:20.[1] A copy of the notification letter is enclosed. MMC also established a dedicated, toll-free call center where notified individuals may obtain more information regarding the incident.

To help prevent something like this from happening in the future, MMC is undertaking a review of how its information is stored with Blackbaud and evaluating Blackbaud's security safeguards.

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

Sincerely,

Eric A. Packel
Partner

Enclosure

[1] This report is not, and does not constitute, a waiver of MMC's objection that New Hampshire lacks personal jurisdiction over MMC regarding any claims related to this data security incident.

Maimonides
Medical Center

<<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>>,

We are contacting you because Maimonides Medical Center ("MMC") was recently informed by Blackbaud, Inc. ("Blackbaud"), a third-party service provider, about a security incident that may have involved your information. Blackbaud provides data hosting services for hundreds of nonprofits globally and large numbers of hospital foundations and universities, including MMC.

What Happened?

MMC uses certain Blackbaud data-solution services in connection with our fundraising activities, and we received notification from Blackbaud that an unauthorized individual had gained access to Blackbaud's systems between February 7, 2020 and May 20, 2020. Blackbaud further advised that the unauthorized individual may have acquired backup copies of databases used by its customers, including a backup of the database we use for fundraising efforts. In response, we took steps to understand the extent of the incident and the data involved.

What Information Was Involved?

On September 25, 2020, our investigation and review of the Blackbaud database involved in the incident determined that it contained your general demographic information and an image of a check used to make a donation, which includes your bank account number and routing number.

Importantly, MMC does **not** store Social Security numbers in the Blackbaud database. This incident did **not** involve any access to our medical systems or electronic health records. Additionally, if you previously made any donations by credit card, Blackbaud has informed us that any credit card information in the database was encrypted, and therefore **not** able to be accessed by the unauthorized individual.

What We are Doing:

MMC takes this event very seriously, and we are evaluating our relationship with Blackbaud and its security safeguards. We also have been advised by Blackbaud that law enforcement authorities have been alerted of this incident.

What You Can Do:

As always, we recommend that you remain vigilant for incidents of fraud, including by regularly viewing your bank account statements. If you see any unusual activity on your bank account statements, please contact your bank.

For More Information:

We regret any inconvenience or concern that this incident has caused you. If you have further questions regarding this matter, please do not hesitate to contact us at 1-833-960-3578 Monday through Friday, from 8:00 am to 5:30 pm, Central Time, excluding major U.S. holidays.

Sincerely,

Sandra C. Maliszewski, MSN, JD, MBA, HCISPP
Vice President, Chief Compliance and Privacy Officer
Maimonides Medical Center

ELN-4834-1120

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. 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:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office,* 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland: 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. You may contact Maimonides Medical Center at 4802 Tenth Avenue, Brooklyn, NY 11219.

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; 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: 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: This incident involves one (1) resident of 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