



Baker&Hostetler LLP

Key Tower
127 Public Square, Suite 2000
Cleveland, OH 44114-1214

T 216.621.0200
F 216.696.0740
www.bakerlaw.com

David E. Kitchen
direct dial: 216.861.7060
dkitchen@bakerlaw.com

October 22, 2020

VIA E-MAIL (NDAG@ND.GOV)

Office of the Attorney General
State Capitol
600 E. Boulevard Ave.
Department 125
Bismarck, ND 58505

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Ronald McDonald House Charities, Upper Midwest (“RMHC-UM”), to notify you of a security incident involving North Dakota residents that was experienced by one of its vendors, Blackbaud, Inc. (“Blackbaud”). Blackbaud is a third-party fundraising software provider used worldwide by thousands of nonprofits, foundations, and others, including RMHC-UM. RMHC-UM is a non-profit patient and family support organization located in Minneapolis, Minnesota.

RMHC-UM was notified by Blackbaud of a ransomware attack on Blackbaud’s network that it discovered in May of 2020. Blackbaud reported that it conducted an investigation of the incident and determined that backup files containing information from some of its clients had been taken from its network. Blackbaud paid a ransom and obtained confirmation that the stolen files had been destroyed. Blackbaud also reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, RMHC-UM conducted its own investigation of the Blackbaud services it uses to determine what information may have been involved in the incident. RMHC-UM determined that a backup of the database previously used to manage RMHC-UM’s guest services may have been accessed or acquired by the unauthorized person. RMHC-UM conducted further review and subsequently identified unencrypted information that may have been viewable in the database pertaining to 2,716 North Dakota residents, including the residents’ names, dates of birth, health insurance information, and/or limited clinical or treatment information, such as healthcare provider names and/or diagnoses or

treatment types. Importantly, Blackbaud assured RMHC-UM that credit card information was not involved in this incident. Additionally, RMHC-UM does not collect Social Security numbers or other financial account information.

Beginning today, October 22, 2020, RMHC-UM is mailing notification letters to the North Dakota residents via First Class US Mail.¹ A sample copy of the notification letter is enclosed. RMHC-UM is recommending that the individuals remain vigilant to the possibility of fraud by reviewing their health account statements for any unauthorized activity. RMHC-UM has also established a dedicated, toll-free number where individuals may obtain more information regarding the incident.

Blackbaud has informed RMHC-UM that they identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect data, and are undertaking additional efforts to improve the security of its environment.

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

Sincerely,

A handwritten signature in blue ink, appearing to read "David E. Kitchen", with a long horizontal line extending to the right.

David E. Kitchen
Partner

Enclosure

¹ This notice does not waive RMHC-UM's objection that North Dakota lacks personal jurisdiction over it related to any claims that may arise from this incident.

Ronald McDonald House Charities,
Upper Midwest / Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



[REDACTED]
[REDACTED]
[REDACTED]

A-62

October 22, 2020

Dear [REDACTED]:

At Ronald McDonald House Charities, Upper Midwest ("RMHC-UM"), we place a high value on maintaining the confidentiality and security of the data we hold. We are writing to inform you about a recent security incident that occurred at Blackbaud, a third-party software provider used worldwide by thousands of schools, foundations, and nonprofits, including RMHC-UM. This notice explains the incident, outlines the measures Blackbaud has taken in response, and provides steps you can take.

What Happened?

Blackbaud recently informed us that it had experienced a security incident that may have involved unauthorized access to a backup of the database we use to manage our guest services. Blackbaud reported that it worked with security experts and law enforcement to conduct an investigation into the incident. Through the investigation, Blackbaud determined that an unauthorized person obtained access to its network between February 7, 2020 and May 20, 2020, and that backup files containing information from its clients had been taken from its network. Blackbaud paid a ransom and obtained confirmation that the files that had been removed, had been destroyed.

Upon learning of the incident from Blackbaud, we immediately conducted our own investigation to understand the extent of the incident and to determine what information may have been involved.

What Information Was Involved?

We determined that the backup file involved may have contained your name, date of birth, and limited clinical or treatment information, such as healthcare provider name and/or diagnosis or treatment type. Importantly, Blackbaud assured us that credit card information was not involved in this incident. Additionally, we do not collect Social Security numbers or other financial account information.

What We Are Doing.

We are notifying you of this incident and sharing the steps that Blackbaud is taking in response. Blackbaud has informed us that they identified and fixed the vulnerability associated with this incident, implemented several changes to better protect data, and are undertaking additional efforts to enhance their security processes.

What You Can Do.

Blackbaud assured us that the backup file has been destroyed by the unauthorized individual and there is no reason to believe any data was or will be misused or disseminated publicly. However, we wanted to notify you of this incident to assure you we take this very seriously. It is always a good idea to review statements you receive from your healthcare provider. If you see any services you did not receive or transactions you do not recognize, you should contact the provider immediately.

For More Information.

We sincerely apologize for any inconvenience or concern this incident may cause. Should you have any further questions regarding this matter, please do not hesitate to call 1-800-403-4529, Monday through Friday, between 8:00 am and 5:00 pm Central Time.

Sincerely,

Ronald McDonald House Charities, Upper Midwest