BakerHostetler

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

September 4, 2020

VIA E-MAIL (NDAG@ND.GOV)

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

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of the University of Missouri – Columbia ("UMC") 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 cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits. UMC uses Blackbaud's data solution services to manage its donor and fundraising information.

On July 16, 2020, Blackbaud informed UMC it discovered that an unauthorized individual had gained access to Blackbaud's systems between February 7 and May 20, 2020. Blackbaud further advised that the unauthorized individual may have accessed or acquired a backup of the database that manages donor information. Blackbaud paid a ransom and obtained confirmation that the files that had been removed had been destroyed. Blackbaud reported that it has been working with law enforcement. UMC immediately took steps to understand the extent of the incident and the data involved.

UMC recently determined that the database that was accessed or acquired by the unauthorized individual may have included the names and dates of birth of 271 North Dakota residents. Blackbaud informed UMC that the fields within the database dedicated to Social Security numbers, financial account information, and payment card information were encrypted, and therefore not accessed or acquired.

Beginning today, UMC is providing written notice via United States Postal Service First-Class mail to the North Dakota residents, in accordance with NDDC § 51-30-05.[1] A copy of the notification letter is enclosed. UMC has provided a phone number where all individuals may obtain more information regarding the incident.

Blackbaud has informed MC that they identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect data from any subsequent incidents, and are undertaking additional efforts to harden their environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.

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

Sincerely,

David E. Kitchen
Partner

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

MIZZOU
OUR TIME TO
LEAD

University of Missouri Advancement
Office of the Vice Chancellor

301 Reynolds Alumni Center
Columbia, MO 65211

573-882-7703 **P**
573-884-5144 **F**

giving.missouri.edu

September 4, 2020

We are writing to inform you that the University of Missouri and many other institutions were recently notified by Blackbaud that it experienced a security incident. This notice explains the incident and measures taken in response. We are notifying you out of an abundance of caution; no additional action is needed from you.

What Happened
Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits. On July 16, 2020, Blackbaud notified us that it had discovered a ransomware attack on Blackbaud's network in May 2020. Blackbaud reported that it conducted an investigation, determined that backup files containing information from its clients had been taken from its network, and an attempt was made to encrypt files to convince Blackbaud to pay a ransom. Blackbaud paid a ransom and obtained confirmation that the files that had been removed had been destroyed. Blackbaud reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, we conducted our own investigation of the Blackbaud services we use and the information provided by Blackbaud to determine what information was involved in the incident. On August 7, we determined that the backup files contained certain information pertaining to you.

What Information Was Involved
The MU data acquired during this incident could have included your public information such as name, date of birth, contact information, degree information and MU giving history. No encrypted data such as Social Security numbers, bank account information, and credit or debit card information was compromised because the University does not store such information. 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 will be disseminated or otherwise made available publicly.

What We Are Doing
We are notifying you of this incident and sharing the steps that we, and Blackbaud, are taking in response. Blackbaud has informed us that they identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect your data from any subsequent incidents, and are undertaking additional efforts to harden their environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.

The university is notifying you out of an abundance of caution. This message does not require any additional action from you. If you think you are the victim of a scam or identity theft, please report it to the appropriate local law enforcement authorities. We apologize for any inconvenience this incident may have caused. If you have further questions, please contact us donorrelations@missouri.edu or 877-738-4546.

Sincerely,
Jackie Lewis
Vice Chancellor for Advancement