GLR
GARLINGTON | LOHN | ROBINSON
MONTANA'S ATTORNEYS SINCE 1870

RECEIVED
DEC - 7 2020
OFFICE OF
ATTORNEY GENERAL

December 3, 2020

***Via USPS & Certified Mail Return Receipt Requested***
North Dakota Office of the Attorney General
600 East Boulevard Avenue, Department 125
Bismarck, ND 58505-0040

RE: UM Foundation and Blackbaud Data Breach Notification

Dear Attorney General Stenehjem:

Garlington, Lohn & Robinson is counsel to the University of Montana Foundation ("UM Foundation"). This letter is meant to notify you of a data security incident that involved Blackbaud, Inc. ("Blackbaud") servers and systems containing UM Foundation data.

Blackbaud is a publicly traded cloud-based software company that caters to nonprofits, foundations, and other juridical entities with a portfolio of products focused on, among other things, fundraising, financial management, and data analytics.

The UM Foundation is a nonprofit organization serving the University of Montana by managing private fundraising efforts, donations, and investment of donations. The UM Foundation is governed by a board of trustees, and operates under an agreement with the University of Montana that is reviewed and approved by the Montana University System Board of Regents.

The UM Foundation uses Blackbaud products and software solutions to manage constituent contacts and further its mission. Blackbaud discovered it had suffered a ransomware attack sometime in May of 2020 and notified UM Foundation of the incident on July 16, 2020. Blackbaud believes the criminal behind the attack did not access any data containing credit card information, bank account information, social security numbers, usernames or passwords. The criminal attempted to encrypt certain other data hosted by Blackbaud systems in order to extort payment for the same data to later be decrypted. During the attack, some personal information belonging to North Dakota residents, believed to be limited to residents' names, addresses, and dates of birth, may have been exposed to the criminal or other individuals.

Blackbaud paid the ransom demanded, conducted its own investigation, alerted law enforcement, and worked with third-party forensic IT consultants to repel the criminal and prevent all of its files from being encrypted. Blackbaud believes the data will not be misused, disseminated or otherwise be made publicly available as a result. Blackbaud's consultants fixed the vulnerability

3084600

P.O. Box 7909 | 350 Ryman St. | Missoula, MT 59807-7909 | PHONE: (406) 523-2500 | FAX: (406) 523-2595 garlington.com
Professional Limited Liability Partnership

203094

that led to the breach, tested the implemented fix against known attack vectors, and are continuing to work with Blackbaud to further secure its network and systems.

The UM Foundation takes this matter seriously and will continue to work closely with Blackbaud to ensure an incident like this does not occur again. The UM Foundation is concurrently notifying its affected North Dakota constituents and the three major credit bureaus of this breach. UM Foundation expects that these affected North Dakota residents will receive letters notifying them of this matter by December 10, 2020. A draft copy of the letter that will be sent to these affected residents is enclosed.

Please contact me should you require additional information regarding this matter.

Sincerely,

GARLINGTON, LOHN & ROBINSON, PLLP

Jason M. Collins
Telephone: 406-523-2500
Email: jmcollins@garlington.com

JMC:dlh
Enclosures

UNIVERSITY OF MONTANA FOUNDATION

December [date], 2020

[Name]
[Address]
[City, State Zip]

RE: Notification of Blackbaud Data Breach Impacting UM Foundation

Dear [Name],

I am writing to let you know about a data security incident experienced by one of our software vendors that may have involved your personal information. The UM Foundation takes the protection and proper use of your information very seriously. We are therefore contacting you to explain what happened, what information was involved, what we are doing, and what you can do to protect your information.

**What Happened**
Blackbaud is a cloud software company that provides cloud software and data services to nonprofit organizations like the UM Foundation. The UM Foundation uses Blackbaud's software and services to support our mission. Blackbaud recently notified us of a security incident in their systems that may have involved your personal information.

Our current understanding is that Blackbaud discovered and stopped a ransomware attack. Ransomware attacks occur when a cybercriminal attempts to steal information and make it inaccessible to its owner by "locking it" with encryption. After discovering the attack, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files. Before Blackbaud expelled the cybercriminal from their system, the cybercriminal removed a copy of Blackbaud's backup file, which may have contained your personal information.

**What Information Was Involved**
It's important to note that Blackbaud's backup file accessed by the cybercriminal did not contain information such as credit card numbers, bank account information, or social security numbers. However, Blackbaud determined that the file removed may have contained names, addresses, and dates of birth.

Blackbaud paid the cybercriminal's demand with confirmation that the copy of Blackbaud's backup file removed by the cybercriminal had been destroyed. Based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigations,

Blackbaud informed us it does not believe any data went beyond the cybercriminal, or that it will be misused, disseminated, or otherwise made publicly available.

**What We Are Doing**

We are notifying you so that you may take action to protect your data. Ensuring the safety of our constituents' data is of the utmost importance to us. As part of its ongoing efforts to help prevent something like this from happening in the future, Blackbaud has already implemented several changes that will protect personal data from future incidents.

Blackbaud explained to us that it was able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and swiftly fixed it. Blackbaud confirmed through testing by multiple third parties that their fix withstands all known attack tactics. Additionally, Blackbaud is accelerating its efforts to further harden its computer systems and network environment.

**What You Can Do**

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to the proper authorities, such as those listed below.

- Federal Trade Commission: ftc.gov or 1-202-326-2222
- Federal Bureau of Investigation: fbi.gov
- North Dakota Attorney General: attorneygeneral.nd.gov or 1-800-472-2600
- Equifax: equifax.com or 1-800-685-1111
- Experian: experian.com or 1-888-397-3724
- TransUnion: transunion.com or 1-888-909-8872

**For More Information**

We regret that one of our software vendors experienced this incident which may have involved your personal information, and for the inconvenience it may cause you. If you have any questions or concerns, please do not hesitate to contact Brad Reardon, UM Foundation Associate Vice President of Information Systems, at 406-243-2593 or brad.reardon@supportum.org.

Sincerely,

Cindy Williams
President and CEO