WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

October 6, 2020

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Email

Attorney General Wayne Stenehjem
Office of the Attorney General
600 East Boulevard Avenue, Department 125
Bismarck, ND 58505-0040
ndag@nd.gov

Re: Data Security Incident

Dear Attorney General Stenehjem:

We represent the North Dakota State University Foundation ("NDSUF"), located at 1241 North University Drive, Fargo, ND 58102, with respect to a data security incident described in more detail below. NDSUF takes the privacy and security of their clients' information very seriously, and has taken steps protect the privacy and security of potentially impacted individuals' information.

1. **Nature of the security incident.**

NDSUF is an advocacy and philanthropy foundation to support North Dakota State University. On Thursday, July 16, 2020, NDSUF received a notification from Blackbaud, Inc. ("Blackbaud") that Blackbaud experienced a cybersecurity incident which resulted in the exposure of personal information maintained by hundreds of non-profit and educational institutions on multiple Blackbaud platforms. As your office may already be aware, Blackbaud is a cloud computing provider that is used by NDSUF and many other institutions to organize and store information related to members of their community, and experienced a ransomware incident in May 2020 which may have resulted in the exposure of personal information maintained by non-profits and educational institutions on Blackbaud platforms ("Blackbaud Incident"). After an initial investigation, NDSUF discovered the Blackbaud platforms they use, called *Raiser's Edge*, *Financial Edge*, and *ResearchPoint*, contained the name, home address, email address, and date of birth of NDSUF donors. According to communication from Blackbaud, Blackbaud did not encrypt these platforms, containing the backup datasets of NDSUF's data.

At this time, based on the information NDSUF received from Blackbaud, NDSUF has no reason to believe that any personal information of any members of the NDSUF community has been or will be misused as a result of this incident.

2. **Number of North Dakota residents affected.**

A total of twenty-seven thousand seven hundred and ninety-one (28,870) North Dakota residents

may have been potentially affected by this incident. A notification letter to these individuals was mailed on October 2, 2020 by first class mail. A sample copy of the notification letter is included with this letter.

3. **Steps taken.**

NDSUF takes the privacy and security of their information very seriously, and has taken steps to protect the privacy and security of potentially impacted individuals' information. Upon discovery of the incident, NDSUF immediately informed Wilson Elser Moskowitz Edelman & Dicker LLP, and began identifying the individuals contained within the *Raiser's Edge*, *Financial Edge,* and *ResearchPoint* platforms in preparation for notice. NDSUF has also requested Blackbaud to explain the steps it has taken to mitigate the risk of a similar attack. Blackbaud has stated that the provider's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix the incident. They have confirmed through testing by multiple third parties, including the appropriate platform vendors, that their fix withstands all known attack tactics. Additionally, they are accelerating our efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

Contact information.

NDSUF remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure.

NDSU | FOUNDATION

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Salutation>>:

We are writing to let you know of a data security incident at a third-party service provider that may have involved some of your personal information. The North Dakota State University Foundation ("Foundation") takes the protection and proper use of your information very seriously; therefore, we are contacting you to explain the incident and measures taken to protect your information. While we do not believe that this incident is reasonably likely to subject you to a risk of harm, we are providing you with this notice in an abundance of caution and transparency.

WHAT HAPPENED?

We were recently notified by one of our vendors, Blackbaud Inc., of a security incident in which Blackbaud experienced a ransomware attack. However, prior to being locked out, the cybercriminals removed backup files from Blackbaud's platform, which hosted data for numerous colleges, universities, health care organizations, foundations, and other non-profit organizations around the world, including the Foundation. Blackbaud believes the incident occurred between February and May 2020. Blackbaud discovered the incident in May, conducted an investigation, and notified the Foundation on July 16, 2020.

WHAT INFORMATION WAS INVOLVED?

After a careful review, we have determined that the information removed by the threat actor may have contained some of your information, which included your name, address and/or date of birth. Please be assured that we do NOT store bank account or credit and debit card information, and therefore none of this information was part of the incident. Blackbaud has confirmed that the investigation found that no encrypted information, such as Social Security numbers or passwords, was accessible. Also, Blackbaud worked with law enforcement and third-party experts and informed us that they paid the threat actor.

RISK AND CONTINUED MITIGATION

At this time, based on the information we have received from Blackbaud, we have no reason 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 continue monitoring for any such activity. Unfortunately, these ransomware attacks are becoming more and more common. As a best practice in today's world of cybercrime, we recommend that you remain vigilant and report any suspicious activity or suspected identity theft to the proper law enforcement authorities. For more information on this incident, please visit ndsufoundation.com/blackbaud.

FOR MORE INFORMATION

We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We sincerely regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact us at privacy@ndsufoundation.com or by calling 701-231-6800.

Sincerely,

John R. Glover

President/CEO
NDSU Foundation

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf) or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.freeze.equifax.com	www.experian.com/freeze	freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.