December 4, 2020

Anjali Das
312.821.6164 (direct)
anjali.das@wilsonelser.com

Via Online Submission

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Data Security Incident

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents University of South Dakota Foundation ("USDF") with respect to a data security incident involving Blackbaud, Inc. (hereinafter, the "Blackbaud Incident") described in more detail below. USDF takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Description of the Blackbaud Incident.

Blackbaud, Inc. ("Blackbaud") is a cloud computing provider that is used by USDF and many other institutions to organize and store information related to members of our community.

On July 16, 2020, as your Office may already be aware, Blackbaud first notified hundreds of its customers, including USDF, that Blackbaud experienced a ransomware event in May 2020 which involved the exposure of data stored by Blackbaud's customers on Blackbaud's platforms. In response to Blackbaud's July notification, USDF launched an internal investigation to determine, based on the information provided by Blackbaud, which of its' constituents were impacted.

Prior to the completion of this investigation, on September 29, 2020, USDF received a second notification letter from Blackbaud (hereinafter, "Blackbaud's September notice"). This letter indicated that it was discovered that additional data maintained by USDF via Blackbaud that was previously believed to be encrypted, was in fact unencrypted and potentially accessible to the threat actor. Following Blackbaud's September notice, USDF continued its internal investigation to determine the identities of additional individuals whose personal information was impacted. During its investigation, USDF discovered that two (2) residents of Maine were impacted by the

Blackbaud incident. Specifically, the Blackbaud Incident resulted in the unauthorized exposure of the Maine residents' personal information, including their tax identification numbers (including social security numbers).

As of this writing, USDF has not received any reports of related identity theft since the date of the incident (May 2020 to present).

2. Number of Maine residents affected.

As discussed above, two (2) residents of Maine were potentially affected. Incident notification letters addressed to those individuals will be mailed on December 4, 2020, via First Class Mail. A sample copy of the Incident notification letters being mailed to potentially affected residents of Maine is included with this letter as **Exhibit A**.

3. Steps taken.

USDF 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, USDF immediately informed Wilson Elser, and began identifying the individuals contained within the Blackbaud platform in preparation for notice. USDF 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 it. 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 their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms. Additionally, all notified individuals were also offered complimentary identity theft and credit monitoring services for a period of twenty-four (24) months.

4. Contact information.

USDF remains dedicated to protecting the sensitive information within 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 AND DICKER LLP

Anjali Das

Anjali Das

EXHIBIT A

UNIVERSITY OF SOUTH DAKOTA FOUNDATION

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

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

<<Date>>

Dear <<Name 1>>:

Please accept this letter as notification of efforts that have taken place at the University of South Dakota Foundation ("USDF") to address notice of a data security incident provided to USDF by Blackbaud, Inc. ("Blackbaud"), a provider of database technologies and cloud computing services.

On July 16th of this year, USDF was among hundreds of institutions notified by Blackbaud of a ransomware attack affecting customer information Blackbaud holds as a service to its largely educational and nonprofit clients. USDF uses a Blackbaud product known as *Financial Edge NXT*, which acts as a database of information gathered about employees and vendors of the University of South Dakota.

Since then, USDF has worked with its insurer to engage outside counsel to further investigate the extent of the breach and its impact on our community. Since we were notified of this incident, we have worked diligently to gather from Blackbaud additional details and understandings of how the incident might have specifically impacted USDF data.

We were notified again on September 29, 2020, that additional personal information of our << Variable Data 3>> was exposed to unauthorized individuals. USDF was notified that your name and <<Breached Elements>> may have been exposed as a result of this incident.

Based on the information we have received from Blackbaud, we have no reason to believe that any personal information of members of the USDF community has been misused as a result of this incident. However, for purposes of full disclosure, we feel it important to inform you that information may have been viewed by unauthorized individuals as a result of this incident. Blackbaud has assured us that appropriate measures have been taken to resolve the incident, strengthen the Blackbaud network, and better secure data stored in the Blackbaud environment.

1110 N. Dakota Street
Vermillion, SD 57069

As a best practice, we recommend that you remain vigilant and report any suspicious activity or suspected identity theft to the proper law enforcement authorities. Please review the enclosed "Additional Important Information" section included with this letter. It explains how you may access a credit monitoring service for two years at no cost to you. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission ("FTC") regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. Please continue to remain vigilant, and carefully monitor your mail and credit reports for any suspicious activity, and report any incident of identity theft to your local law enforcement, Attorney General, and the FTC.

We remain in contact with Blackbaud to promote accountability and to better understand their corrective solutions. We regret any inconvenience this situation may cause. Should you have any further questions or concerns regarding this letter, please contact us at 605-624-5709 or usdfound@usdfoundation.org. You may also visit our website at usdalumni.com/blackbaud.

Sincerely,

Steve Brown,
President & CEO

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For *residents* of *Arizona, Colorado, Maryland, Rhode Island, Illinois, New York,* and *North Carolina*:
You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.
Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us
Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com
Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft
Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov
Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025
Illinois Office of the Attorney General Consumer Protection Division 100 W Randolph St., Chicago, IL 60601 1-800-243-0618 www.illinoisattorneygeneral.gov

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

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);TransUnion (https://www.transunion.com/fraud-alerts); 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
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

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

Blackbaud Credit Monitoring Service

Blackbaud is providing you with access to **Single Bureau Credit Monitoring*** services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

Proactive Fraud Assistance. For sensitive breaches focused on customer retention, reputation management, or escalation handling, CyberScout provides unlimited access during the service period to a fraud specialist who will work with enrolled notification recipients on a one-on-one basis, answering any questions or concerns that they may have. Proactive Fraud Assistance includes the following features:

- Fraud specialist-assisted placement of fraud alert, protective registration, or geographical equivalent, in situations where it is warranted.
- After placement of a Fraud Alert, a credit report from each of the three (3) credit bureaus is made available to the notification recipient (United States only).
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Answering any questions individuals may have about fraud.
- Provide individuals with the ability to receive electronic education and alerts through email. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Identity Theft and Fraud Resolution Services. Resolution services are provided for enrolled notification recipients who fall victim to an identity theft as a result of the applicable breach incident. ID Theft and Fraud Resolution includes, but is not limited to, the following features:

- Unlimited access during the service period to a personal fraud specialist via a toll-free number.
- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparation of all documents needed for credit grantor notification, and fraud information removal purposes.
- All phone calls needed for credit grantor notification, and fraud information removal purposes.
- Notification to any relevant government and private agencies.
- Assistance with filing a law enforcement report.
- Comprehensive case file creation for insurance and law enforcement.
- Assistance with enrollment in applicable Identity Theft Passport Programs in states where it is available and in situations where it is warranted (United States only).
- Assistance with placement of credit file freezes in states where it is available and in situations where it is warranted (United States only); this is limited to online-based credit freeze assistance.
- Customer service support for individuals when enrolling in monitoring products, if applicable.
- Assistance with review of credit reports for possible fraudulent activity.
- Unlimited access to educational fraud information and threat alerts. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Enrollment Instructions

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please navigate to:

https://www.cyberscouthq.com/epiq263?ac=263HQ796

If prompted, please provide the following unique code to gain access to services: **263HQ796**

Once registered, you can access Monitoring Services by selecting the "Use Now" link to fully authenticate your identity and activate your services. Please ensure you take this step to receive your alerts within 90 days from the date of this letter.