LEWIS BRISBOIS BISGAARD & SMITH LLP

Kamran Salour
650 Town Center Drive, Suite 1400
Costa Mesa, California 92626
Kamran.Salour@lewisbrisbois.com
Direct: 714.966.3145

December 10, 2020

File No. 30841.1177

VIA ELECTRONIC MAIL ONLY

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504
E-Mail: SecurityBreach@atg.wa.gov

Re: **Notice of Data Security Incident**

Dear Attorney General Ferguson:

We represent the Oklahoma State University Foundation ("OSUF") in connection with the recent data security incident experienced by Blackbaud, Inc. ("Blackbaud"), one of the largest providers of fundraising and financial management software for non-profit organizations, including OSUF. The incident did not involve OSUF's network or systems. OSUF recently determined that the incident Blackbaud experienced involved personal information for OSUF constituents. Following this determination, OSUF has notified the affected individuals and provided them with steps they can take to protect their personal information.

I. Nature of the Security Incident

On July 16, 2020, Blackbaud reported that it experienced a data security incident that may have involved information pertaining to OSUF community members. Upon learning of the incident, OSUF immediately launched an investigation to determine what happened and whether any personal information was impacted. According to Blackbaud, between February 7, 2020 and June 4, 2020, an unauthorized party had access to backup files related to the Blackbaud fundraising and donor management software that used by OSUF.

Upon learning this information, OSUF retained outside cybersecurity experts to conduct an investigation. During the course of the investigation, OSUF determined that personal information for OSUF constituents was contained in the backup files. On August 7, 2020, OSUF sent an email to all constituents to inform them of the incident.

Recently, OSUF was able to identify the constituents whose regulated data sets were contained in the backup files. Accordingly, on December 10, 2020, OSUF provided individual notification letters to these constituents and provided them with steps they can take to protect their personal information.

II. Type of Information and Number of Washington Residents Involved

The incident involved personal information for 1,334 Washington residents. The information involved in the incident may differ depending on the individual but may include name, address, phone number, email address, date of birth, gender, giving information, and publicly-available donor analytics data. For OSU alumni, the information involved may also include degree information and membership in student organizations.

III. Steps Taken Relating to the Incident

As soon as OSUF learned of the incident, it launched an investigation. It also worked with Blackbaud to obtain additional information regarding the incident and to confirm that the company was taking steps to ensure that the information at issue was not being misused, and that it was taking steps to further protect OSUF information going forward. Blackbaud has represented that they are monitoring the dark web for any exchange of personal information related to this incident, but have found no indication that the information is available on the dark web. Blackbaud also stated that they have reported the incident to the Federal Bureau of Investigation (FBI). OSUF will provide the FBI and law enforcement whatever assistance is needed. In addition, OSUF has notified the affected individuals and provided them with steps they can take to protect their personal information.

IV. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at Kamran.Salour@lewisbrisbois.com or 714.966.3145.

Sincerely,

Kamran Salour of
LEWIS BRISBOIS BISGAARD & SMITH LLP

KS

Enclosure: Notification Letter Template

OKLAHOMA STATE UNIVERSITY
FOUNDATION

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 10, 2020

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

As a member of the Oklahoma State University Cowboy Family, we wanted to follow up on an email we sent you in August letting you know about a data security incident experienced by Blackbaud, Inc., a third-party service provider for the OSU Foundation, that may have involved your personal information. We appreciate the sensitive nature of this information, and we want to keep you informed about what occurred. This letter contains additional information we have learned since our email and website notice and provides steps you can take to protect your personal information.

What Happened: On July 16, 2020, Blackbaud informed us that it had experienced a data security incident that may have involved information pertaining to our alumni and donors. Upon learning of the incident, we immediately engaged our own cybersecurity experts and launched an investigation to determine what happened and what information may have been impacted. Through the course of our investigation, we learned that between February 7, 2020, and May 20, 2020, an unauthorized third party gained access to Blackbaud's servers where backup files for our fundraising and donor relationship management software were stored. Our investigation determined that some of your personal information was contained in the backup files. Blackbaud has informed us that it has no reason to believe that any information in the files has been or will be misused or will otherwise be made available publicly.

What Information Was Involved: The incident may have involved the following information: name, address, phone number, email address, date of birth, gender, giving information, and publicly available donor analytics data. For OSU alumni, the information involved may have also included degree information and membership in student organizations. Please be assured that your Social Security number, bank account number, and credit/debit card information were NOT involved in the incident. The Foundation does not and did not store any of this information on the affected systems

What We Are Doing: As soon as we learned of the incident, we engaged our own cybersecurity experts and launched an investigation. We also worked with Blackbaud to obtain additional information regarding the incident, to confirm that information for our donors and alumni was not misused, and to ensure that it took steps to further protect this information going forward. We also confirmed that the incident was reported to the Federal Bureau of Investigation, and we will offer the FBI whatever assistance is needed to hold the perpetrators accountable. In addition, we are notifying you of the incident and providing you with steps you can take to protect your personal information.

What You Can Do: Please review the information included with this letter for steps to protect your personal information.

For More Information: If you have any questions about this letter, please call 800-939-4170 between 8:00 a.m. and 5:00 p.m. Central Time. You may also consult the resources included on the following page, which provides information about how to protect your personal information.

The security of your information is a top priority for OSU and the Foundation. We are committed to safeguarding your data and being transparent should issues like this arise. Our ability to ensure the Cowboy family stays connected through every generation relies on trust, and we take this responsibility very seriously.
Sincerely,

Blaire Atkinson, President
Oklahoma State University Foundation

Steps to help Protect your Information

1. Review your credit reports. We encourage you to remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit

reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Information regarding an IDX Identity Protection Membership

1. Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using the Enrollment Code provided at the bottom of the letter.

2. Activate the credit monitoring provided as part of an IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.