Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

October 22, 2020

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent the University of Nevada, Las Vegas Foundation ("UNLV Foundation") located at 4505 S. Maryland Parkway, Las Vegas, Nevada 89154, and are writing to notify your office of an incident that may affect the security of some personal information relating to two thousand five hundred and sixty-three (2,563) Washington residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the UNLV Foundation does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about Thursday July 16, 2020, the UNLV Foundation received notification of a cyber incident from one of its third-party vendors, Blackbaud Inc. ("Blackbaud"). Blackbaud reported that, in May 2020, it experienced a cyber attack incident that resulted in encryption of certain Blackbaud systems. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain customer data stored on its system at some point before Blackbaud locked the cybercriminal out of the system in May 2020. Following the notification from Blackbaud, the UNLV Foundation immediately began an investigation to determine the nature and scope of the incident, including what, if any, sensitive UNLV Foundation data was potentially involved. On September 10, 2020, after a thorough review process, the UNLV Foundation confirmed that legally protected personal information may have been present in the involved Blackbaud systems at the time of the incident. Thereafter the UNLV Foundation

continued to work to confirm the appropriate contact information and provide legal notice to potentially affected individuals were required as quickly as possible.

The information that could have been subject to unauthorized access includes name, date of birth, and/or student identification number.

Notice to Washington Residents

On October 22, 2020, the UNLV Foundation provided written notice of the Blackbaud incident to two thousand five hundred and sixty-three (2,563) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon receiving notice from Blackbaud, the UNLV Foundation moved quickly to investigate and respond to the incident, and assess the security of UNLV Foundation systems. The UNLV Foundation sent preliminary notice to its constituents in August of 2020 while it continued gathering information from Blackbaud. The UNLV Foundation is reviewing its existing policies and procedures regarding its third-party vendors, and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

In addition to the preliminary notice, the UNLV Foundation is providing legal notice to individuals whose personal information was potentially impacted by the Blackbaud event. The UNLV Foundation provided notified individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. The UNLV Foundation is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,

Sian M Schafle

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/smm

EXHIBIT A

UNLV | FOUNDATION

Return Mail Processing Center
P.O. 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>>:

The University of Nevada, Las Vegas Foundation ("UNLV Foundation") writes to inform you of a recent incident that may affect the privacy of some of your information. On Thursday, July 16, 2020, the UNLV Foundation received notification from Blackbaud, Inc., a third-party vendor contracted by the UNLV Foundation ("Blackbaud"), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including the UNLV Foundation. Blackbaud is a leading provider of data services in the academic sector, and a vendor of the UNLV Foundation for nearly 25 years. Upon receiving notice of the cyber incident, we immediately began an investigation to better understand the nature and scope of the incident and any impact on UNLV Foundation data. While we understand that you may have received a prior notification from the UNLV Foundation back in early August, our further investigation determined that you are legally due notice of this event because of the specific personal information related to you potentially impacted as a result of this event. Accordingly, this notice provides you with information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

Blackbaud reported that, in May 2020, it experienced a cyber attack incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain customer data stored on its system at some point before Blackbaud locked the cybercriminal out of the system in May 2020. Upon learning of the Blackbaud incident, the UNLV Foundation immediately began our investigation to determine what, if any, sensitive UNLV Foundation data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. During this process, the UNLV Foundation worked extensively with cybersecurity incident response specialists and Blackbaud to ensure a full understanding of the potentially impacted UNLV Foundation information. On September 10, 2020, after a thorough review process, the UNLV Foundation confirmed that legally protected personal information as defined by your state may have been present in the involved Blackbaud systems at the time of the incident. Thereafter we continued to work to confirm the appropriate contact information and provide this legal notice to potentially affected individuals where required as quickly as possible.

Specifically, our investigation determined that the involved Blackbaud systems contained your name and <<Breached Elements>>. Please note that, to date, we have not received any information from Blackbaud that your information was specifically accessed or acquired by the unknown actor, and we are unaware of any actual or attempted misuse of your personal information as a result of this incident. Blackbaud has also informed us that **no** Social Security numbers, financial account numbers, or credit card numbers were compromised as part of this incident.

The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying government regulators, as required.

We encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information.

We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at 855-914-4635, which is available Monday through Friday between 6:00 a.m. and 6:00 p.m. PT.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Tiffany L. Vickers

Tiffany L. Vickers
Senior Associate Vice President, Finance and Administration
Chief Financial Officer
University of Nevada, Las Vegas Foundation

Steps You Can Take to Help Protect Your Information

Monitor Accounts

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. Law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Ave. NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.