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

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

September 4, 2020

VIA E-MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Drake University, located at 2507 University Ave, Des Moines, IA 50311, and are writing to notify you of an incident that may affect the security of the personal information of certain Washington residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to this submission. By providing this notice, Drake University does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

Nature of the Data Event

On July 16, 2020, Drake University was notified by its third-party vendor, Blackbaud, that between February and May 2020, Blackbaud experienced a data security incident that resulted in the unauthorized acquisition of data impacting a large group of the organizations to whom they provide services, including Drake University. Blackbaud is a cloud software provider that provides Drake University and many other nonprofit organizations and educational institutions with database and relationship management services.

In its initial communication, Blackbaud reported that, in May 2020, it experienced a ransomware 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 Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Upon receiving notice from Blackbaud, Drake University began its own internal investigation into the information reported by Blackbaud and the impact on data maintained in the impacted systems on behalf of Drake University. Based on the Drake University ongoing investigation, on August 5, 2020, it was determined the personal information that could have been subject to unauthorized access or acquisition included names and dates of birth.

Notice to Washington Residents

Drake University began providing notice of this incident to one thousand and fifty (1,050) Washington residents on September 4, 2020, in substantially the same form as the notice attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Promptly after Blackbaud notified Drake University of the issue, it took steps to determine its nature and scope, including whether any personal information was impacted. Drake University continues to investigate this issue in coordination with Blackbaud. Blackbaud reported that it is making enhancements to its systems to help detect and prevent unauthorized access to information, including (1) hardening its controls related to access management, network segmentation, and endpoint and network-based protection; and (2) accelerating its efforts to strengthen its password requirements and implement multi-factor authentication for its self-hosted solutions. Blackbaud also reported that it has engaged third-party experts to actively monitor its systems for suspicious activity. In addition, Drake University understands that Blackbaud has consulted with law enforcement on this issue. Based on the investigation, and the information received from Blackbaud, at this time, Drake University has no evidence that any of the information has been misused as a result of this issue.

Additionally, Drake University is providing impacted 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. Drake University 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/amw
Enclosure

EXHIBIT A

Drake
UNIVERSITY

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 4, 2020

F7657-L01-0000001 P001 T00001 **********MIXED AADC 159
SAMPLE A SAMPLE
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A Sample:

We are writing to notify you that Drake University was recently informed of an incident that may have involved some of your information. This letter explains the incident, our response, and resources available to you to help protect your information from possible misuse.

On Thursday, July 16, 2020, Drake University received notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident. Drake University uses Blackbaud to provide fundraising and relationship management services through its RaisersEdge product. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Drake University data.

Blackbaud reported that, in May 2020, it experienced a ransomware 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 Blackbaud customer data before Blackbaud locked the threat actor out of the environment on May 20, 2020. Drake's investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On or about August 5, 2020, Drake University's investigation determined that the information potentially affected may have contained personal information.

Our investigation determined that the involved Blackbaud systems contained your name and impacted data 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. Blackbaud reported that Social Security number, credit card information and financial account numbers were not impacted as a result of this event. Moreover, Drake University does not store this type of information in the Blackbaud's systems.

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 Drake's 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 state and federal 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.

0000001

We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 800-626-4089 Monday-Friday, 9 a.m.–12 p.m. & 1–4 p.m. CT. You may also write to Drake University at 2507 University Ave, Des Moines, IA 50311.

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

Sincerely,

John P. Smith, AS’92, GR’00
Vice President, University Advancement

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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
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 Avenue 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.