Lynda Jensen
Office: (267) 930-2303
Fax: (267) 930-4771
Email: Ljensen@mullen.law

430 Franklin Village Dr, #184
Franklin, MA 02038

December 11, 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 Fairfield University located at 1073 N Benson Road, Fairfield, Connecticut 06824, and are writing to notify your office of an incident that may affect the security of some personal information relating to five hundred five (505) Washington residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Fairfield University 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

Fairfield University received notice from its third-party vendor, Blackbaud, Inc. ("Blackbaud"), regarding a data security event that occurred in May 2020 and 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. Specifically, Blackbaud reported that certain data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of its environment on May 20, 2020. Upon learning of the Blackbaud incident, Fairfield University commenced an investigation to determine what, if any, sensitive Fairfield University data may have been involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On or about September 30, 2020, Fairfield University received further information from Blackbaud regarding the scope and types of information

potentially affected by the incident. Through its review of the information Blackbaud provided, Fairfield University determined on November 12, 2020 that the information potentially affected by the Blackbaud incident included the following types of information relating to Washington residents: name and date of birth.

Notice to Washington Residents

On or about December 11, 2020, Fairfield University began providing written notice of this incident to affected individuals, which includes five hundred five (505) 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 of the event, Fairfield University moved quickly to obtain additional information from Blackbaud required to appropriately investigate and respond. Fairfield University is also working to review its existing policies and procedures regarding third-party vendors and working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

Additionally, Fairfield 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. Fairfield 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) 930-2303.

Very truly yours,

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ:mf1

EXHIBIT A

Fairfield UNIVERSITY

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

December 11, 2020

G0458-L01-0000001 T00017 P003 *********ALL FOR AADC 123
SAMPLE A SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A Sample,

Fairfield University writes to inform you of a recent incident that may affect the privacy of some of your information. On Thursday, July 16, 2020, Fairfield University received notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), regarding a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Fairfield University. 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 Fairfield University data. This notice provides 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 it experienced a ransomware incident in May 2020 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. Specifically, Blackbaud reported that certain data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of its environment on May 20, 2020. Upon learning of the Blackbaud incident, Fairfield University commenced an investigation to determine what, if any, sensitive Fairfield University data may have been involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On or about September 30, 2020, Fairfield University received further information we requested from Blackbaud and promptly began reviewing that information to understand the scope and types of information potentially affected by the incident. Through our review of the further information Blackbaud provided, on November 12, 2020, we determined that the information potentially affected by the Blackbaud incident included your name and date of birth. Please note that, to date, we have not received confirmation from Blackbaud that the unknown actor accessed or acquired your specific information.

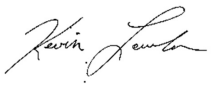
The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information entrusted to us, we are working to review our existing policies and procedures regarding our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

Although we have no evidence of actual misuse of your information as a result of incident, if you believe it is appropriate, you may review the enclosed *Steps You Can Take to Help Protect Your Information* for general information about 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 call our dedicated assistance line at (888) 994-0284 toll-free Monday through Friday from 8 am – 10 pm Central time, or Saturday and Sunday from 10 am – 7 pm Central time (excluding major U.S. holidays). Be prepared to provide your engagement number DB24297. You may also write to Fairfield University ATTN: Kevin Lawlor at 1073 N Benson Road, Fairfield, CT 06824.

We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,



Kevin Lawlor
Executive Vice President and Chief Operating Officer

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:

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

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

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 years, 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.); and
7. If you are a victim of identity theft, 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 seven-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.

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

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 19106
1-800-680-7289
https://www.transunion.com/fraud-alerts

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); and 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.