MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Julie Siebert-Johnson
Office: (267) 930-4005
Fax: (267) 930-4771
Email: jsjohnson@mullen.law

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

March 11, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Blackbaud Data Event

Dear Sir or Madam:

We represent The Buckley School ("Buckley") located at 113 E. 73rd Street, New York, New York 10021 and write to notify your Office of an incident that may affect the privacy of some personal information relating to approximately six (6) New Hampshire residents. This notice may be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, Buckley does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

Blackbaud is a cloud computing provider that provides financial services tools to organizations and schools, including Buckley. On July 16, 2020, Buckley received notification from Blackbaud of a cyber incident on its network. 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. Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data from Blackbaud's network at some point before Blackbaud locked the unknown actor out of the environment on May 20, 2020. While Blackbaud discovered this activity in May 2020, it was not until July 16, 2020 that Blackbaud notified Buckley that an unknown actor may have accessed or acquired certain Blackbaud customer data. When Blackbaud first notified Buckley in July, Blackbaud reported that certain information, such as Social Security numbers, financial information and credit card information, were encrypted within the Blackbaud systems and, therefore, were not accessible to the unknown actor.

Upon receiving notice from Blackbaud, Buckley immediately commenced an investigation to better understand the incident and any impact on Buckley data. This investigation included working diligently to gather further information from Blackbaud. On November 6, 2020, following several requests to

Blackbaud, Buckley received updated information related to the event. Buckley promptly began a thorough review of the information provided by Blackbaud to determine what, if any, sensitive information was contained on the Blackbaud system at the time of the event. Upon completing its initial review, Buckley identified a number of individuals for whom address information could not be located. Therefore, Buckley conducted an extensive manual review of source documents and internal records to correctly identify the requisite address information. Buckley completed its review on February 10, 2021. The type of information impacted by Blackbaud's event varied by individual but may have included the following: name and financial account information.

Notice to New Hampshire Residents

On March 11, 2021, Buckley provided written notice of this incident to approximately six (6) New Hampshire residents. Written notice was provided in substantially the same form as the letter attached hereto as ***Exhibit A***. To date, Buckley has not received any information from Blackbaud that any Buckley information was specifically accessed or acquired by the unknown actor.

Other Steps Taken and To Be Taken

Upon discovering the event, Buckley moved quickly investigate and respond to the incident. Buckley is reviewing its existing procedures regarding its third-party vendors and is working with Blackbaud to ensure additional measures and safeguards are in place to protect against this type of incident in the future. Further, Buckley is offering individuals access to complimentary credit monitoring services through CyberScout for 24 months.

Additionally, Buckley is providing individuals with guidance on how to better protect against identity theft and fraud, including 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) 930-4005.

Very truly yours,

Julie Siebert-Johnson of
MULLEN COUGHLIN LLC

JSJ/jc1
Enclosure

EXHIBIT A

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>>

Re: Notice of Blackbaud Data Security Incident

Dear <<Name 1>>,

The Buckley School ("Buckley") writes to notify you of the Blackbaud, Inc. ("Blackbaud") data security incident because we believe your data may have been affected. Blackbaud is a cloud computing provider that provides financial services tools to organizations and schools, including Buckley. To date, Blackbaud has not reported that your information has been misused as a result of this incident. Nevertheless, we are notifying you so that you are aware of the incident and may take steps to better protect your information, should you feel it appropriate to do so.

What Happened? On July 16, 2020, we received notification from Blackbaud of a cyber incident on its network. 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. Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data from Blackbaud's network at some point before Blackbaud locked the unknown actor out of its systems on May 20, 2020. When Blackbaud first notified us in July, Blackbaud reported that certain information, such as Social Security numbers, financial information, and credit card information, was encrypted within the Blackbaud systems and not accessible to the unknown actor.

Upon receiving notice from Blackbaud, we immediately commenced an investigation to better understand the incident and any impact on Buckley data. This investigation included working diligently to gather further information from Blackbaud. Following several requests to Blackbaud, we received updated information related to the event. We immediately began a thorough review of the information provided by Blackbaud to determine what, if any, sensitive information was contained on the Blackbaud system at the time of the event. On February 10, 2021, we completed our review of impacted information and confirmed contact information for potentially impacted individuals.

What Information Was Involved? Our investigation determined that the involved Blackbaud systems contained your name and <<Data Elements>>. Please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by an unknown actor, nor has Blackbaud reported any actual or attempted misuse of Buckley information.

What Are We Doing? The security of information in our care is among our highest priorities. As part of our ongoing commitment to the security of information, we are working to review our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to confirm additional measures and safeguards are in place to protect against this type of incident in the future.

Although we are unaware of any actual or attempted misuse of your information as a result of this incident, we are offering you access to credit monitoring and identity protection services through CyberScout HQ for 24 months at no cost to you as an added precaution. A description of services and instructions on how to enroll can be found within the enclosed "*Steps You Can Take to Help Protect Your Information.*" Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. Please review the enclosed "*Steps You Can Take to Help Protect Your Information*" for general information on what you can do to help protect your personal information.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, we established a dedicated assistance line at 866-800-6743 which can be reached Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. You may also contact us by mail at 113 E. 73rd Street, New York, New York 10021. Protecting your information is important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Thomas Stanton
Chief Financial Officer

Steps You Can Take to Help Protect Your Information

Enroll in Credit Monitoring

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

https://www.cyberscouthq.com/ [redacted]

If prompted, please provide the following unique code to gain access to services: [redacted]

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.**

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud and to monitor your accounts/free credit reports for suspicious activity and to detect errors. 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	Chester, PA 19016	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 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, 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 one 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 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.

This notice has not been delayed by law enforcement.

For Rhode Island residents, the Rhode Island Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 4 Rhode Island residents impacted by this incident.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023 or 1-888-743-0023, and www.oag.state.md.us. Buckley may also be contacted by mail at The Buckley School 113 E. 73rd Street New York, NY 10021.

For 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 violators. 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. We encourage you to 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.

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

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, and www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Washington, D.C. residents, the Office of Attorney General for the District of Columbia can be contacted at 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; and https://oag.dc.gov.