MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Michael J. Bonner
Office: (267) 930-4815
Fax: (267) 930-4771
Email: mbonner@mullen.law

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

September 28, 2020

VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent The Lexington School ("Lexington") located at 1050 Lane Allen Road, Lexington, Kentucky and write to notify your Office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. This notice may be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, Lexington 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

On July 16, 2020, Lexington received a communication from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Lexington.

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 what occurred. Following its investigation, Blackbaud notified its customers, including Lexington, that an unknown actor may have accessed or acquired certain Blackbaud customer data.

Blackbaud reported that the data was accessed or acquired by the unauthorized actor at some point before Blackbaud locked the unauthorized actor out of the environment on May 20, 2020.

Upon receiving notice of the cyber incident, Lexington immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Lexington data. This investigation included working diligently to gather information from Blackbaud to understand the scope of the incident. On August 13, 2020, Lexington received further information regarding the Blackbaud event that allowed it to confirm the information potentially affected may have contained personal information. Based on this information, Lexington undertook an investigation to determine what information may have been present in the system. On August 17, 2020, following an extensive review of its files, Lexington determined that personal information relating to certain individuals was present on Blackbaud's system at the time of the event. The type of information potentially impacted for the New Hampshire resident included name and Social Security number.

Notice to New Hampshire Resident

On September 28, 2020, Lexington provided written notice of this incident to affected individuals, which include one (1) New Hampshire resident. 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 discovering the event, Lexington moved quickly to investigate and respond to the incident and to notify potentially affected individuals. This included coordination with Blackbaud to confirm what information may have been affected by Blackbaud's incident. Lexington is reviewing existing policies and procedures regarding third-party vendors and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

Additionally, Lexington is providing potentially impacted individuals access to credit monitoring services for 12 months through Kroll. Lexington is also providing 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. Lexington 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. Lexington is also notifying state regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4815

Very truly yours,

Michael J. Bonner of
MULLEN COUGHLIN LLC

Encl.

EXHIBIT A

The Lexington School

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

The Lexington School ("TLS") writes to notify you of the recent Blackbaud, Inc. ("Blackbaud") data security incident because we believe your data may have been affected. Blackbaud provides data services to us and thousands of other private schools and nonprofits worldwide. 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.

On July 16, 2020, TLS received notice from Blackbaud of a cybersecurity event that occurred on their systems that was discovered in May of 2020. The notice advised that a subset of data was taken from the Blackbaud systems, including data potentially related to TLS. On August 13, 2020, TLS received further information regarding the Blackbaud event that allowed it to confirm the information potentially affected may have contained personal information. While Blackbaud has not confirmed what data specifically relating to TLS was involved in the event, it advised that backup copies of data were accessed or acquired during the event. Based on this information, we undertook an investigation to determine what information may have been present in the Blackbaud system. On August 17, 2020, following an extensive review of our files, TLS determined that personal information relating to certain individuals, including you, was present on Blackbaud's system at the time of the event. The type of information included the following data elements: <<b2b_text_1 (Impacted Data)>>.

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 evaluate additional measures and safeguards 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 identity monitoring services through Kroll for twelve (12) months at no cost to you as an added precaution. A description of services and instructions on how to activate can be found within the enclosed "Steps You Can Take to Safeguard Your Personal Information." Please note that you must complete the activation process yourself, as we are not permitted to activate you in these services on your behalf.

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 1-866-394-1255 which can be reached Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. You may also contact TLS by mail at 1050 Lane Allen Road, Lexington, KY 40504. Protecting your information is important to us, and TLS remains committed to safeguarding the information in our care.

Sincerely,

S.T. O'Brien
Chief Financial Officer

Steps You Can Take to Safeguard Your Personal Information

Activate Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **December 22, 2020** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud. 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 2000
Chester, PA 19016
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

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 2002
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
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), 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 reached 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 **[XX]** Rhode Island residents impacted by this incident.

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 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 reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.