



MULLEN  
COUGHLIN<sub>LLC</sub>  
ATTORNEYS AT LAW

RECEIVED

FEB 05 2021

CONSUMER PROTECTION

Ryan C. Loughlin  
Office: (267) 930-4786  
Fax: (267) 930-4771  
Email: rloughlin@mullen.law

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

January 26, 2021

**VIA U.S. MAIL**

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

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Long Island Lutheran Middle and High School (“LuHi”) located at 131 Brookville Road, Glen Head, New York 11545, and are writing to notify your office of an incident that may affect the security of some personal information relating to two (2) New Hampshire 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, LuHi 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**

LuHi’s third-party vendor, Blackbaud Inc. (“Blackbaud”) reported to LuHi that it experienced an attempted ransomware incident in May 2020 that impacted 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’s investigation determined that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reports that data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. LuHi received a second notification from Blackbaud on September 29, 2020, stating that this incident impacted personal information related to LuHi. Upon receiving this second notification, LuHi immediately commenced an investigation to determine what, if any, sensitive LuHi data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident.

The information that could have been subject to unauthorized access includes name, address, and Social Security number.

### **Notice to New Hampshire Residents**

On or about January 26, 2021, LuHi provided written notice of this incident to affected individuals, which includes two (2) New Hampshire 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**

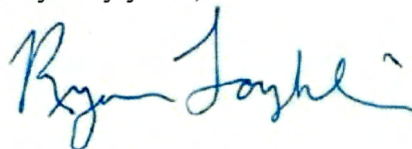
LuHi is providing access to credit monitoring services for two (2) years, through CyberScout, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, LuHi 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. LuHi 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. LuHi is also providing written notice of this incident to other state regulators, as necessary.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,

A handwritten signature in blue ink that reads "Ryan Loughlin". The signature is fluid and cursive, with a small mark at the end.

Ryan C. Loughlin of  
MULLEN COUGHLIN LLC

RCL/kjc  
Enclosure

# **EXHIBIT A**



Return Mail Processing Center  
PO 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>>:

Lutheran High School Association of Nassau and Suffolk Counties (“LuHi”) writes to inform you of a recent incident at our third-party vendor, Blackbaud, Inc. (“Blackbaud”), that may affect the privacy of some of your information. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including LuHi. This notice provides information about the Blackbaud incident, LuHi’s response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

**What Happened?** Blackbaud reported to LuHi that it experienced an attempted ransomware incident in May 2020 that impacted 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’s investigation determined that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reports that data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. LuHi received a second notification from Blackbaud on September 29, 2020, stating that this incident impacted personal information related to LuHi. Upon receiving this second notification, LuHi immediately commenced an investigation to determine what, if any, sensitive LuHi data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident.

**What Information Was Involved?** Our investigation, and that of Blackbaud, determined that the involved Blackbaud systems contained your name and <<Data Elements>>.

**What We Are Doing.** 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 are also offering you access to complimentary credit monitoring and identity protection services for 24 months through CyberScout. These services include fraud consultation and identity theft restoration services. Enrollment instructions can be found in the enclosed *Steps You Can Take to Help Protect Your Information*.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information*. There you will also find more information on the credit monitoring and identity protection services we are making available to you.

**For More 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 800-690-5157 between the hours of 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday.

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

Sincerely,

Lutheran High School Association of Nassau and Suffolk Counties



## ***STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION***

We are providing you with access to **Single Bureau Credit Monitoring** services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud, you will also have access to remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

**Proactive Fraud Assistance.** For sensitive breaches focused on customer retention, reputation management, or escalation handling, CyberScout provides unlimited access during the service period to a fraud specialist who will work with enrolled notification recipients on a one-on-one basis, answering any questions or concerns that they may have.

**Identity Theft and Fraud Resolution Services.** Resolution services are provided for enrolled notification recipients who fall victim to an identity theft as a result of the applicable breach incident.

### **How do I enroll for the free services?**

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.**

In order for you to receive the monitoring services described above, you must enroll by March 27, 2021.

### **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 (1) free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://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](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-298-0045

[www.equifax.com/personal/credit-report-services](http://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](http://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](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com/personal/  
credit-report-services](http://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](http://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.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023; 410-576-6300.

**New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**North Carolina Residents:** Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC).