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

January 19, 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 Staten Island Academy ("SIA") located at 715 Todt Hill Road, Staten Island, New York 10304 and write to notify your Office of an incident that may affect the security of some personal information relating to approximately 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, SIA 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 database service tools to organizations and schools, including SIA. On, July 16, 2020, SIA 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 threat actor out of the environment on May 20, 2020. In its July 16, 2020 notice, 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 threat actor.

Upon receiving notice from Blackbaud, SIA immediately commenced an investigation to better understand the incident and any impact on SIA data. This investigation included working diligently to gather further information from Blackbaud. On September 29, 2020, more than two months after first notifying SIA, Blackbaud notified SIA again, and stated that, contrary, to its previous representations, certain Social Security numbers and vendor information may have been affected by the Blackbaud incident. Blackbaud reported that at some historical point, this information had been transferred into an unencrypted state

without SIA's knowledge. Following this update, SIA requested additional information from Blackbaud to confirm the individuals whose sensitive information may have been stored on a Blackbaud systems at the time of the incident as some of the systems identified by Blackbaud are no longer used by SIA. On December 7, 2020, Blackbaud began providing the necessary information from Blackbaud. However, the updated information provided by Blackbaud lacked sufficient contact information for several individuals, and, as such, SIA commenced a thorough review of its internal records to identify all potentially impacted individuals. On December 31, 2020, SIA received the remaining necessary information from Blackbaud and completed its internal review at which time SIA confirmed the population of potentially impacted individuals. SIA thereafter worked to provide notice to potentially impacted individuals as quickly as possible.

The information that could have been subject to unauthorized access includes information as defined by New Hampshire law including name and Tax ID number.

Notice to New Hampshire Resident

On January 19, 2021, SIA provided written notice of this incident to approximately one (1) New Hampshire resident. Written notice was provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, SIA moved quickly investigate and respond to the incident, to assess the security of SIA systems, and to notify potentially affected individuals. SIA is reviewing its existing procedures regarding its third-party vendors, and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. Further, in coordination with Blackbaud SIA is offering individuals access to complimentary credit monitoring services through CyberScout for twenty-four (24) months to individuals whose personal information was potentially affected by this incident at no cost to these individuals.

Additionally, SIA 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. SIA 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) 930-4005.

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: <<Variable Header>>

Dear <<Name 1>>:

Staten Island Academy ("SIA") writes to make you aware of an incident involving one of our third-party vendors, Blackbaud, Inc. ("Blackbaud") that may affect the privacy of some of your information. *While we have no evidence of any actual or attempted misuse of any information as a result of this incident*, this notice provides information about the Blackbaud incident, our response and efforts to obtain additional information from Blackbaud, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On Thursday, July 16, 2020, SIA received notification from Blackbaud of a cyber incident on its network. Blackbaud is a cloud computing provider that provides financial services tools to organizations and schools, including SIA. 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 threat 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 SIA that an unknown actor may have accessed or acquired certain Blackbaud customer data. When Blackbaud first notified SIA 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, therefore, was not accessible to the threat actor. SIA relied on these assertions to determine that this information had not been impacted by the Blackbaud incident.

Upon receiving notice from Blackbaud, SIA immediately commenced an investigation to better understand the incident and any impact on SIA data. This investigation included working diligently to gather further information from Blackbaud. On September 29, 2020, more than two months after first notifying SIA, Blackbaud notified SIA again and stated that, contrary to its previous representations, certain Social Security numbers and vendor information may have been affected by the Blackbaud incident. Blackbaud reported that at some historical point, this information had been transferred into an unencrypted state without SIA's knowledge. Following this update, SIA requested additional information from Blackbaud to confirm the individuals whose sensitive information may have been stored in a Blackbaud systems at the time of the incident. Because this information was not accessible to SIA, we were reliant upon Blackbaud to provide the list of individuals whose unencrypted information was present on Blackbaud's network at the time of the incident. On December 7, 2020, Blackbaud began providing the necessary information. However, the updated information provided by Blackbaud lacked sufficient contact information for several individuals and, as such, we commenced a thorough review of our internal records to identify all potentially impacted individuals. On December 31, 2020, we received the remaining necessary information from Blackbaud and completed our internal review which confirmed your information was among those that may have been impacted. We thereafter worked to provide notice to potentially impacted individuals as quickly as possible.

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 SIA information.

What Are We 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 reviewing our existing procedures regarding our third-party vendors. SIA is continuing to work with Blackbaud to address relevant questions and next steps Blackbaud is taking to remediate its data privacy event. Please note that Blackbaud confirmed it will be removing this historical unencrypted SIA information from its network. We will also be notifying state regulators, as required.

Further, although SIA is unaware of any actual or attempted misuse of your information as a result of this incident, as an added precaution, and at no cost to you, we are providing you with access to credit monitoring services through CyberScout for 24 months. A description of these services and instructions on how to enroll can be found in 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. We encourage you to remain vigilant against incidents of fraud or identity theft and to monitor your accounts and free credit reports for suspicious activity and to detect errors. Please also 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 that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please contact us at 800-532-9322, Monday through Friday, from 9 am to 9 pm Eastern Time, (excluding some U.S. national holidays). You may also write to Staten Island Academy at 715 Todt Hill Road, Staten Island, New York 10304.

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

Sincerely,

Albert R. Cauz
Head of School

Jacqueline M. Anzurez
Chief Financial Officer

Arthur Grinev
Director of Technology

Steps You Can Take to Help Protect Your Information

Enroll in Monitoring Services

As an added precaution, and at no cost to you, we are providing you with access to **Single Bureau Credit Monitoring*** in this matter. Services are for 24 months from the date of enrollment. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

To enroll in Credit Monitoring services, please visit: **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.**

ADDITIONAL INFORMATION REGARDING YOUR 24-MONTH MONITORING PRODUCT

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. Proactive Fraud Assistance includes the following features:

- Fraud specialist-assisted placement of fraud alert, protective registration, or geographical equivalent, in situations where it is warranted.
- After placement of a Fraud Alert, a credit report from each of the three (3) credit bureaus is made available to the notification recipient (United States only).
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Answering any questions individuals may have about fraud.

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. ID Theft and Fraud Resolution includes, but is not limited to, the following features:

- Unlimited access during the service period to a personal fraud specialist via a toll-free number.
- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparation of all documents needed for credit grantor notification, and fraud information removal purposes.
- All phone calls needed for credit grantor notification, and fraud information removal purposes.
- Notification to any relevant government and private agencies.
- Assistance with filing a law enforcement report and comprehensive case file creation for insurance and law enforcement.
- Assistance with placement of credit file freezes in states where it is available and in situations where it is warranted (United States only); this is limited to online-based credit freeze assistance.
- Customer service support for individuals when enrolling in monitoring products, if applicable.
- Assistance with review of credit reports for possible fraudulent activity.

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 (3) 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	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

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 one (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	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	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	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); or 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. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023 or 410-576-6300; www.oag.state.md.us.

For New York residents, the New York Attorney General provides resources regarding identity theft protection and security breach response at www.ag.ny.gov/internet/privacy-and-identity-theft. The New York Attorney General may be contacted by phone at 1-800-771-7755; toll-free at 1-800-788-9898; or online at www.ag.ny.gov.