MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Vincent F. Regan
Office: (267) 930-4842
Fax: (267) 930-4771
Email: vregan@mullen.law

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

March 9, 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 The Galloway Schools, Inc. ("TGS") located at 215 Chastain Park Avenue NW, Atlanta, Georgia 30342, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, TGS 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 Thursday, July 16, 2020, TGS was among many organizations across the country notified that one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), was the target of a cyber incident. Blackbaud is one of the most commonly utilized cloud computing providers that offers customer relationship management and financial services tools for many independent schools, universities, and non-profit organizations. TGS itself was not the target of this incident and did not experience any compromise of its own systems.

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 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. Blackbaud reported that certain data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment. Unfortunately, Blackbaud's incident impacted a significant number of organizations, including TGS.

Upon learning of the Blackbaud incident, TGS immediately commenced an investigation to determine what, if any, sensitive TGS data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. TGS worked to confirm the type of information involved, and to whom that information pertained and determined that the information that could have been subject to unauthorized access includes name, address, and financial account information of one (1) New Hampshire resident.

Notice to New Hampshire Resident

On or about March 9, 2021, TGS provided written notice of this incident to all affected individuals, which includes 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, TGS moved quickly to investigate and respond to the incident, assess the security of TGS systems, and notify potentially affected individuals. TGS is also working to implement additional safeguards and training to its employees. TGS is providing access to credit monitoring services for one (1) year, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, TGS 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. TGS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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) 930-4842.

Very truly yours,

Vincent F. Regan of
MULLEN COUGHLIN LLC

VFR/eeb
Enclosure

EXHIBIT A

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

March 9, 2021

G2987-L03-0000002 T00001 P001 *****AUTO**MIXED AADC 159
SAMPLE A. SAMPLE - L03-PERSONAL
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789

Re: Notice of Security Breach

Dear Sample A. Sample:

The Galloway School ("TGS") writes to inform you of a recent incident at one of our third-party vendors that may affect the privacy of some of your information. This notice provides information about the incident, our response, 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, TGS was among many organizations across the country notified that one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), was the target of a cyber incident. Blackbaud is one of the most commonly utilized cloud computing providers that offers customer relationship management and financial services tools for many independent schools, universities, and non-profit organizations. TGS itself was not the target of this incident and did not experience any compromise of its own systems.

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 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. Unfortunately, Blackbaud's incident impacted a significant number of organizations, including TGS.

Upon learning of the Blackbaud incident, TGS immediately commenced an investigation to determine what, if any, sensitive TGS data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident, and to confirm the type of information involved, and to whom that information pertained.

What Information is Involved? The information related to you and maintained by Blackbaud that may have been impacted includes your name and [DATA_ELEMENTS]. This information most likely was stored as a result of a donation you made several years ago.

What Are We Doing? We take the security of information entrusted to us very seriously and apologize for the inconvenience this incident has caused. We are also notifying state regulators, as required.

What You Can Do. As a best practice, 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 Protect Personal Information.* Although we are not aware of any actual or attempted misuse of your personal information, as an added precaution we have arranged to offer you access to 12 months of complimentary credit monitoring and identity protection services provided through Experian. Although we are making these services available to you, we are unable to enroll you directly. For enrollment instructions, please review the information contained in the attached *Steps You Can Take to Protect Personal Information.*

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at **(833) 541-1361** toll-free Monday through Friday from 9 am – 11 pm Eastern time, or Saturday and Sunday from 11 am – 8 pm Eastern time (excluding major U.S. holidays) and be prepared to reference engagement number **DB25814**. You may also write to TGS at: 215 Chastain Park Avenue NW, Atlanta, Georgia 30342.

Sincerely,

Veronique Kessler
CFO, The Galloway School

Paige Smith
Director of Development, The Galloway School

Steps You Can Take to Protect Personal Information

Enroll in Credit Monitoring

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **May 31, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGH1**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 541-1361** by **May 31, 2021.** Be prepared to provide engagement number **DB25814** as proof of eligibility for the identity restoration services by Experian.

Monitor Accounts

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:

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	1-800-685-1111
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 (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	**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. 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, 1-410-528-8662, www.oag.state.md.us. You may write to TGS at: 215 Chastain Park Avenue NW, Atlanta, Georgia 30342. *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, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft. *For 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/. *For District of Columbia residents*, the Office of the District of Columbia Attorney General can be contacted at 400 6th Street, NW, Washington, DC 20001; Phone (202) 727-3400; Fax: (202) 347-8922; TTY: (202) 727-3400; Email: oag@dc.gov; or you may visit the website of the Office of the District of Columbia Attorney General at https://oag.dc.gov/.