150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

March 22, 2021

Bruce A. Radke
312-463-6211
312-819-1910 Direct Fax
bradke@polsinelli.com

Via Email (ATTORNEYGENERAL@DOJ.NH.GOV)

Attorney General Gordon J. MacDonald
Office of the Attorney General
Attn: Security Incident Notification
33 Capitol Street
Concord, NH 03301

Re: Notification of a Computer Security Incident Involving Personal Information Pursuant to N.H. Rev. Stat. § 359-C:20

Dear Attorney General MacDonald:

We represent Millbrook School ("Millbrook") in connection with an incident that may have impacted the personal information of five (5) New Hampshire residents, and provide this notice on behalf of Millbrook pursuant to N.H. Rev. Stat. § 359-C:20(I)(b). We will supplement this notice, if necessary, with any new significant facts discovered subsequent to its submission. While Millbrook is notifying you of this incident, Millbrook does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY INCIDENT

Millbrook contracts with Blackbaud, Inc. ("Blackbaud") to manage its databases within Blackbaud's self-hosted environment. On July 16, 2020, Blackbaud notified Millbrook that Blackbaud was impacted by a ransomware event in May 2020. In its original communication, Blackbaud informed Millbrook that it encrypted Millbrook's sensitive data contained within Blackbaud's systems. However, on October 20, 2020, Blackbaud notified Millbrook that it discovered the personal information, including certain student, donor and vendor data, that Blackbaud previously believed to be encrypted was unencrypted and accessible to the unauthorized third party.

Upon learning of the potentially unencrypted personal information, Millbrook promptly began an internal review of the files that had been stored within Blackbaud's environment to determine

which individuals were potentially impacted by the incident. However, as a result of the COVID-19 pandemic and local health and safety ordinances, Millbrook focused its resources on preventing a COVID-19 outbreak on its campus. Once Millbrook confirmed the health and safety of its campus, Millbrook completed its review of the files stored in Blackbaud's environment.

Soon after, Millbrook determined that the incident impacted certain individuals' personal information, including, depending on the individual, their name, Social Security number, or tax identification number. Millbrook then began locating addresses for the potentially impacted individuals, and conducted an analysis of applicable state data breach notification laws to determine if notice of the incident was required. After determining its notification obligations, Millbrook worked to identify the potentially impacted individuals' contact information and worked with a mailing vendor to notify the individuals.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Millbrook is notifying the potentially impacted five (5) New Hampshire residents by letter today, March 22, 2021. Enclosed is a copy of the notice that is being sent to the New Hampshire residents via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

In addition to notifying the potentially impacted five (5) New Hampshire residents, Millbrook is providing them with information on how they can protect themselves against fraudulent activity and identity theft, and offering the individuals, with impacted Social Security numbers, twenty-four (24) months of complimentary credit monitoring and identity theft services. Finally, Millbrook is reviewing its relationship with Blackbaud and the technical controls in place for securing Millbrook's data in the Blackbaud system.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Bruce A. Radke

Enclosure

MILLBROOK SCHOOL

[redacted]

Dear [redacted]:

Millbrook School ("Millbrook") values and respects the privacy of your information, which is why we are writing to advise you of a recent data security incident involving a company called Blackbaud, Inc. ("Blackbaud"). Millbrook, like thousands of other schools, foundations, and non-profits, contracts with Blackbaud to manage our donor and vendor databases. We have no reason to believe your personal information has been misused for the purpose of committing fraud or identity theft. Nonetheless, we are writing to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

On July 16, 2020, Blackbaud notified us that it was impacted by a ransomware event. According to Blackbaud, in May 2020, an unauthorized third party attempted to deploy ransomware within Blackbaud's environment. Blackbaud was able to prevent the ransomware from deploying, but the threat actor was able to exfiltrate some data out of its systems.

In its original communication to us, Blackbaud informed us that it encrypted most of the data it stores, including Social Security numbers. However, on or around October 20, 2020, Blackbaud informed us that it discovered that the personal information it previously thought was encrypted prior to the incident, was actually unencrypted and potentially accessible to the unauthorized third party. The newly discovered unencrypted information was contained in a database not known to Millbrook and we were not previously aware of its existence. After receiving this additional information from Blackbaud, we determined that the incident may have impacted some of your personal information, including your name and Social Security number.

We take our responsibility to safeguard personal information seriously and apologize for any inconvenience or concern this incident might cause. Upon learning of the incident, we worked with Blackbaud to obtain additional information about the nature of the event. Although we are not aware of any instances of fraud or identity theft, we are offering through Blackbaud a complimentary two-year membership of Single Bureau Credit Monitoring from CyberScout, LLC ("CyberScout"). This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Single Bureau Credit Monitoring through CyberScout is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and Single Bureau Credit Monitoring through CyberScout, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter.**

[redacted]

We are committed to taking steps to help prevent this from happening again, including reviewing our relationship with Blackbaud and the technical controls they have in place for securing our data. If you have any questions, please call a toll-free response line we set up with a third-party to answer your questions at [redacted], Monday through Friday, 8 a.m. to 5 p.m. Eastern Time.

Sincerely,

[redacted]

[redacted]

Credit Monitoring Enrollment

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 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.

How do I enroll for the free services?
To enroll in Credit Monitoring services at no charge, please navigate to:
[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 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. 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.
- Provide individuals with the ability to receive electronic education and alerts through email. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

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.
- Comprehensive case file creation for insurance and law enforcement.
- Assistance with enrollment in applicable Identity Theft Passport Programs in states where it is available and in situations where it is warranted (United States only).

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.
Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.
This notice was not delayed due to a law enforcement delay.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Washington, DC Residents: Washington, DC residents can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.