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

December 3, 2020

Michael J. Waters
312.463.6212
312.873.2918 Fax
mwaters@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 Moses Brown School ("Moses Brown") in connection with an incident that involved the personal information of one (1) New Hampshire resident, and provide this notice on behalf of Moses Brown pursuant to N.H. Rev. Stat. § 359-C:20(I)(b). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Moses Brown is notifying you of this incident, Moses Brown 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 OR UNAUTHORIZED ACCESS

Moses Brown contracts with Blackbaud, Inc. ("Blackbaud") to manage its donor database within Blackbaud's self-hosted environment. On July 16, 2020, Blackbaud notified Moses Brown that it was impacted by a ransomware event in May 2020. Blackbaud prevented the ransomware from deploying, but the unauthorized third party exfiltrated data, including some of Moses Brown's student, donor, and vendor data, out of Blackbaud's systems starting on or around April 18, 2020 through May 7, 2020. In this original communication, Blackbaud informed Moses Brown that it encrypted the sensitive data contained within its systems. However, on October 23, 2020, Blackbaud notified Moses Brown that it discovered the personal information, it previously believed to be encrypted prior to the incident, was unencrypted and accessible to the unauthorized third party.

Upon learning of the potentially unencrypted information, Moses Brown determined that the incident impacted certain individuals' personal information, including, depending on the individual, their name and either their Social Security number or tax identification number.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Moses Brown determined that the incident potentially impacted one (1) New Hampshire resident. Moses Brown notified the potentially impacted New Hampshire resident of the incident by letter today. Enclosed is a copy of the notice that Moses Brown sent to the impacted individual.

STEPS TAKEN RELATING TO THE INCIDENT

Upon becoming aware of the incident, Moses Brown promptly investigated the incident to determine what, if any, personal information a third party might have accessed or acquired during the incident. Moses Brown provided complimentary identity theft protection services, through Blackbaud, to the impacted individuals and provided the individuals with information on how they can protect themselves against fraudulent activity and identity theft.

CONTACT INFORMATION

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

Sincerely,

Michael J. Waters

Enclosure

250 Lloyd Avenue Providence, Rhode Island 02906-2398 ☏ 401.831.7350 🖷 401.455.0084 💻
www.mosesbrown.org

Moses Brown School

December 3, 2020

[redacted]

Dear [redacted]

Moses Brown School ("Moses Brown") 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"). Moses Brown contracts with Blackbaud to manage our donor, alumni, and vendor databases within Blackbaud's self-hosted environment.

Blackbaud recently notified us, as well as hundreds of other organizations that use its products, that it was impacted by a ransomware event. According to Blackbaud, in May 2020, an unauthorized third party deployed ransomware within Blackbaud's environment and some of its data was exfiltrated out of its systems. On or around October 23, 2020, Blackbaud informed us that the unauthorized individual who gained access to Blackbaud's network could have accessed files that contained your name and tax identification number ("TIN"). In addition, if you use your Social Security number as your TIN, as it relates to your professional engagement with Moses Brown, your Social Security number may have also been impacted by the incident. **At this point, we have received no indication that any such information has been misused for fraud or identity theft.** Nonetheless, we are providing you with this notice because your personal information may have been affected by the incident.

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 through 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.**

We value the trust you place in us and take our responsibility to safeguard your personal information seriously. We apologize for any inconvenience or concern this incident might cause. 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. For further assistance, please call [redacted], from [redacted], Monday through Friday.

Sincerely,

[redacted]

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: 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 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).
- 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.
- Unlimited access to educational fraud information and threat alerts. (Note that these emails may not be specific to the recipient's jurisdiction/location)

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.

You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	Trans Union 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

In order to request a security freeze, you may 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.); and
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.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

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.

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.

Rhode Island Residents: We believe that this incident affected 736 Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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).