



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

RECEIVED

DEC 11 2020

CONSUMER PROTECTION

Sian M. Schafle  
Office: (267) 930-4799  
Fax: (267) 930-4771  
Email: [sschafle@mullen.law](mailto:sschafle@mullen.law)

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

November 18, 2020

**VIA FIRST-CLASS MAIL**

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

**Re: Notice of the Blackbaud Data Event**

Dear Sir or Madam:

We represent Metairie Park Country Day School ("MPCDS") located at 300 Park Rd, Metairie, LA 70005, and are writing to notify your office of an incident that may affect the security of some personal information relating to approximately two (2) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MPCDS 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 financial services tools to organizations and schools, including MPCDS. On July 16, 2020, MPCDS received notification from Blackbaud of a cyber incident that occurred on Blackbaud's network. Blackbaud reported that it experienced a ransomware incident in May 2020 that resulted in encryption of certain Blackbaud systems. Blackbaud advised that it reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Blackbaud reported that the threat actor was able to exfiltrate 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 MPCDS that an unknown actor may have accessed or acquired certain Blackbaud customer data. When Blackbaud first notified MPCDS of this incident, it reported that certain information, such as Social Security numbers, were encrypted within the Blackbaud systems and, therefore, were not accessible to the threat actor.

On September 29, 2020, more than two months after first notifying MPCDS of the incident, Blackbaud notified MPCDS again, and stated that, contrary to its previous representations, certain information previously believed to be encrypted and, thus, inaccessible to the threat actor was in fact accessible during the period of unauthorized activity on the network. Blackbaud reported that this information had been transferred into an unencrypted state at some time in the past without MPCDS's knowledge. As such, this

information may have been accessible to the threat actor. MPCDS immediately investigated this expanded scope to confirm the individuals to whom this information related. Blackbaud reported that it could not rule out unauthorized acquisition of MPCDS data. Because this information was not accessible to MPCDS in the database, the school was reliant upon Blackbaud to provide the list of individuals whose information was present on Blackbaud's network at the time of the incident.

On October 19, 2020, Blackbaud provided this updated information, at which time, MPCDS confirmed that it included name, address, and Social Security number for certain New Hampshire residents. Thereafter, MPCDS worked to confirm the appropriate contact information and provide notice to potentially impacted individuals as quickly as possible.

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

On or about November 18, 2020, MPCDS began providing written notice of this incident to affected individuals, which includes approximately 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**

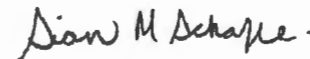
Upon discovering the event, MPCDS moved quickly to investigate and respond to the incident, to assess the security of MPCDS systems, and to notify potentially affected individuals. MPCDS is reviewing its existing policies and procedures regarding its third-party vendors, and is working with Blackbaud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

Additionally, MPCDS is providing impacted 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.

#### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,



Sian M. Schafle of  
MULLEN COUGHLIN LLC

# Exhibit A



METAIRIE PARK COUNTRY DAY

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: Notice of Data <<Variable Data>>

Dear <<Name 1>>:

Metairie Park Country Day School ("MPCDS") writes to inform you of a recent incident involving one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), that may have affected 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, MPCDS 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 MPCDS. 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. Blackbaud reported that the threat actor was able to exfiltrate 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 MPCDS that an unknown actor may have accessed or acquired certain Blackbaud customer data. When Blackbaud first notified MPCDS of this incident, it reported that certain information, such as Social Security numbers, were encrypted within the Blackbaud systems and, therefore, were not accessible to the threat actor. MPCDS relied on these assertions to assure certain members of its community in August 2020 that this information had not been impacted by the Blackbaud incident.

Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on MPCDS data. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident and to assess the risk to any MPCDS data stored on impacted systems. On or about September 9, 2020, MPCDS received further information from Blackbaud about this incident and the scope of the impact to MPCDS data. At that time, Blackbaud was not able to confirm if any MPCDS data has been subject to unauthorized access or acquisition, but Blackbaud stated that it could not rule out that possibility. However, Blackbaud also reiterated that certain data fields, including Social Security number, were encrypted and inaccessible to the threat actor as a result of this event.

On September 29, 2020, more than two months after first notifying MPCDS, Blackbaud notified MPCDS again, and stated that, contrary to its previous representations, certain Social Security numbers may have been subject to unauthorized access or acquisition. Blackbaud reported that at some historical point, these Social Security numbers had been transferred into an unencrypted state without MPCDS's knowledge and this information may have been accessible to the threat actor. MPCDS immediately investigated this expanded scope to confirm the individuals to whom this information related. Because this information was not accessible to MPCDS, we were reliant upon Blackbaud to provide the list of individuals whose unencrypted Social Security numbers were present on Blackbaud's network at the time of the incident. On October 19, 2020, Blackbaud provided this updated information, at which time we confirmed your Social Security number was among those that may have been impacted.

**What Information Was Involved?** Our investigation determined that the potentially impacted personal information included your name and Social Security number. Please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by an unknown actor.

**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 working to review our existing procedures regarding our third-party vendors. MPCDS 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 MPCDS information from its network. We will also be notifying state regulators, as required.

Further, although MPCDS 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 for 24 months in this matter. 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 identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information and a description of services and instructions on how to enroll in these services.

**For More Information.** We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If so, please contact our toll-free dedicated assistance line at 855-914-4689, 9:00 am to 9:00 pm Eastern Time Monday through Friday (excluding some U.S. national holidays). You may also write to Metairie Park Country Day School at 300 Park Rd, Metairie, LA 70005 or email us at [bonnie\\_lagraize@mpcds.com](mailto:bonnie_lagraize@mpcds.com).

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

Sincerely,



Bonnie LaGraize  
Chief Financial Officer  
Metairie Park Country Day School

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

### **Enroll in Credit Monitoring**

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 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. This notice has not been delayed by law enforcement.

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  
1-800-685-1111  
[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  
1-888-766-0008  
[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.

**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; and <https://ag.ny.gov/>. **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](http://www.ncdoj.gov). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft. **For Rhode Island residents**, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is approximately **one (1)** Rhode Island resident impacted by this incident.

