BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

ONE EASTOVER CENTER
100 VISION DRIVE, SUITE 400
JACKSON, MISSISSIPPI 39211

P.O. BOX 14167
JACKSON, MISSISSIPPI 39236

PHONE: 601.351.2400
FAX: 601.351.2424

www.bakerdonelson.com

BRAD C. MOODY
Direct Dial: 601.351.2420
Direct Fax: 601.592.2420
E-Mail Address: bmoody@bakerdonelson.com

December 29, 2020

Attorney General Gordon J. MacDonald
Office of New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: *Charleston Day School - Notice of Vendor Data Incident*

Dear Attorney General MacDonald:

I serve as outside legal counsel to Charleston Day School ("CDS"), which is a coeducational, private, independent K-8 school in Charleston, South Carolina.[1] CDS is located at 15 Archdale Street, Charleston, South Carolina 29401. CDS does not maintain any physical presence or facilities in your State.

This correspondence is to notify you of a recent security incident involving Blackbaud, Inc. ("Blackbaud"), an outside vendor of CDS.[2] On July 16, 2020, CDS was notified that Blackbaud had discovered and stopped a ransomware attack on Blackbaud's self-hosted platform in May of 2020.[3] Blackbaud is the global market leader in third-party, not-for-profit applications used by many charitable and educational organization.

According to Blackbaud, prior to being locked out, the cybercriminal removed a copy of a subset of data from its self-hosted environment which contained information related to individuals affiliated with multiple charitable institutions. Blackbaud reports that it paid the cybercriminal's demand and received confirmation that the copy of the data removed has been destroyed. According to Blackbaud, this incident occurred at some point between February 7, 2020 and May 20, 2020 and was discovered in May of 2020.

Blackbaud recently provided CDS new information regarding the incident and alerted CDS that personal information for some of its constituents may have been impacted by this incident. CDS immediately began reviewing its records to determine what information may have been

[1] By providing this notice, CDS does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the Massachusetts data event notification statute, or personal jurisdiction.

[2] Blackbaud's headquarters are located at 65 Fairchild Street, Charleston, South Carolina 29492.

[3] Blackbaud reported that it notified the FBI of this incident.

impacted and if it needed to notify any of its constituents. CDS' review required it to carefully examine records to identify what information was contained in the files that Blackbaud stated were subject to the attack.

Because Blackbaud reported that a subset of Blackbaud's customer data may have been impacted by the incident, in an abundance of caution, notification letters are being sent via U.S. Mail to one (1) resident of your State on or about December 29, 2020. The data that was potentially impacted may have included the individual's name and Social Security number. A sample notification letter is enclosed for your reference and includes:

- A description of the security incident;
- Steps taken to investigate;
- Steps taken to mitigate any potential harm to constituents or vendors;
- Instructions for activation of 2 years of free credit monitoring and identity theft protection services to all consumers who received notification;
- Instructions on how to place a security freeze on the recipient's consumer credit report; and
- Instructions regarding how to obtain more information about this incident,

Based on the nature of the incident, Blackbaud's research, and third-party investigation, including investigation by law enforcement, Blackbaud has stated that it has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly. In addition to implementing numerous security changes, Blackbaud reports that it has hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

CDS is fully committed to protecting consumer privacy and has certain protocols for information security and safeguarding information. Please contact me if you require any additional information regarding this vendor incident.

Best regards,

BAKER, DONELSON, BEARMAN,
CALDWELL & BERKOWITZ, PC

Brad C. Moody

Enclosure:

Exhibit 1: Sample Notification Letter sent to 1 resident

Charleston Day School

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

RE: Notice of Third-Party Data Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a recent security incident involving Blackbaud, Inc., which provides software and services to Charleston Day School, that may have affected some of your personal data.

What Happened?

Blackbaud, a global market leader in third-party applications used by many charities, health, and educational organizations in the U.S. and abroad, notified us that it discovered and stopped a ransomware attack of its self-hosted platform earlier this year. According to Blackbaud, after discovering the attack, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement— successfully prevented the cybercriminal from blocking Blackbaud's system access and fully encrypting files; and ultimately expelled the cybercriminal from Blackbaud's system.

Prior to being locked out of Blackbaud's system, the cybercriminal removed a copy of a subset of data from its self-hosted environment that contained information related to individuals affiliated with multiple charitable and non-profit institutions. Blackbaud reports that it paid the cybercriminal's demand and received confirmation that the copy of the data removed has been destroyed. You may have been notified by us previously regarding this incident. However, Blackbaud has since investigated further and amended its initial findings about the scope of the incident. We are providing this notice to you out of an abundance of caution.

What Information Was Involved?

Blackbaud recently provided new information to us regarding the incident and alerted us that personal information for some of our constituents may have been impacted by this incident. We immediately began reviewing our records to determine what information may have been impacted and if we needed to notify any of our constituents. Our review required us to carefully examine records to identify what information was contained in the files that Blackbaud stated were subject to the attack, and we began the process of notifying individuals as quickly as possible once we confirmed this information.

According to Blackbaud, your name, address and social security number may have been involved in the incident.

Based on the nature of the incident, Blackbaud's research, and third-party investigation, including investigation by law enforcement, Blackbaud has stated that it has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly. Additionally, Blackbaud reports it has hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

What Are We Doing?

Ensuring the safety of our constituents' data is of the utmost importance to us. For your peace of mind, Blackbaud is offering you two (2) years of credit monitoring at no charge. In order for you to receive these monitoring services, you must enroll within 90 days from the date of this letter. The activation instructions are included with this notification.

Additionally, we are reviewing all relevant practices regarding the security of Blackbaud data. Blackbaud reported that it has implemented numerous security changes. Blackbaud stated that it quickly identified the vulnerability associated with this incident and took swift action to fix it. Blackbaud stated that it has confirmed through testing by multiple third parties that its fix withstands all known attack tactics. Finally, Blackbaud asserted that it is further hardening its environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

What Can You Do?

While Blackbaud has stated that it has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly, we still recommend you take precaution and activate the free credit monitoring. Also, we have included some additional steps that you can take to protect yourself, as you deem appropriate.

For more information about this incident, you can consult the Blackbaud website at www.blackbaud.com/securityincident. If you have additional questions about this incident, please call 1-833-960-3582 toll free Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time (excluding holidays). Thank you for your partnership and continued support.

Kind Regards,

Heidi S. Whaley

Heidi S. Whaley
Chief Business Officer

STEPS YOU CAN TAKE

- **Below is information on steps you can take to protect yourself.**

Blackbaud is 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.

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.)

Enrollment Instructions

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.

Below are additional actions you may take, if you feel it is necessary.

➢ **FREEZE YOUR CREDIT FILE.** You have a 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. Note that a security freeze generally does not apply to existing account relationships and when a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a security freeze.

To place a security freeze on your credit report, contact each of the three major consumer reporting agencies using the contact information listed below:

3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.), Social Security number, and date of birth;
- If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
- 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.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus 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 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 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 a 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 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 the request to remove the freeze.

➢ **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit 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 an alert lasting 7 years. Contact the credit reporting agencies listed above to activate an alert.

➢ **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS, & REPORT FRAUD**. Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity. Report suspicious or fraudulent charges to your insurance statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor and law enforcement. (For Oregon & Iowa residents: Report any suspected identity theft to law enforcement, Federal Trade Commission, and your State Attorney General.)

➢ **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain one free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

➢ **POLICE REPORT:** You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it.

➢ **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM FTC / STATE ATTORNEY GENERAL.** Go to http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html. The Federal Trade Commission also provides information at www.ftc.gov/idtheft. The FTC can be reached by phone: 1 - 877-438-4338; TTY: 1-866-653-4261 or by writing: 600 Pennsylvania Ave., NW, Washington, D.C. 20580. Your State Attorney General also may provide information. For Maryland residents: You may contact Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023. For North Carolina residents: You may contact North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

➢ **FILE YOUR TAXES QUICKLY AND SUBMIT IRS FORM 14039.** If you believe you are at risk for taxpayer refund fraud, the IRS suggests you file your income taxes quickly. Additionally, if you are an actual or potential victim of identity theft, the IRS suggests you give them notice by submitting IRS Form 14039 (Identity Theft Affidavit). This form will allow the IRS to flag your taxpayer account to alert them of any suspicious activity. Form 14039 may be found at https://www.irs.gov/pub/irs-pdf/f14039.pdf.

➢ **FAIR CREDIT REPORTING ACT:** You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Please note that identity theft victims and active duty military personnel may have additional rights under the FCRA.

➢ **PROTECT YOURSELF FROM PHISHING SCAMS.** Learn to recognize phishing emails. Do not open emails from unknown senders and be sure not to click on strange links or attachments. Never enter your username and password without verifying the legitimacy of the request by contacting the sender by telephone or other methods. Replying to the email is not a safe way to confirm. Visit https://www.consumer.ftc.gov/articles/0003-phishing for more information on these types of scams.