[redacted]

CARY ACADEMY

December 11, 2020

[redacted]

Re: Notice of Third-Party Vendor Data Incident

Dear [redacted],

We are writing to notify you that Blackbaud, Inc. ("Blackbaud"), one of our outside vendors, recently made us aware of a data security incident that may have affected some of your personal data. Cary Academy takes the protection and proper use of your information very seriously. Accordingly, in an abundance of caution, we wanted to notify you of this incident and how you may be impacted.

What happened?

We were notified by Blackbaud that it discovered and stopped a ransomware attack upon its self-hosted platform in May 2020. Blackbaud is a global market leader in third party applications used by many universities, charities, health care organizations, foundations, and other educational organizations in the U.S. and abroad.

According to Blackbaud, upon discovery of the attack, its Cyber Security team, together with independent forensics experts and law enforcement, successfully prevented the cybercriminal from blocking access to Blackbaud's system and fully encrypting files. Prior to locking the cybercriminal out, Blackbaud reported that the cybercriminal removed a copy of a subset of data from its self-hosted environment. Blackbaud reports that it paid the cybercriminal's ransom 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 Blackbaud originally made us aware of this incident on July 16, 2020.

On September 29, 2020, and again on October 22, 2020, Blackbaud provided new information regarding the incident and alerted us that personal information from some of Cary Academy's constituents and vendors may have been impacted by the incident. We immediately began reviewing our records and the information provided by Blackbaud to determine what information may have been impacted and if we needed to notify any of our constituents and vendors. Our review required us to manually examine records to determine what information may have been contained in the files that Blackbaud states were subject to the attack. On November 16, 2020, we determined that some of your information may have been impacted.

What information was involved?

Based upon the information provided by Blackbaud, your first and last name 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 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. Blackbaud has hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

What are we doing?

We take the issue of data security very seriously. For your peace of mind, Blackbaud is offering you two (2) years of free credit monitoring at no charge. **In order to receive these credit monitoring services, you must enroll within 90 days from the date of this letter**. The activation instructions are included with this notification.

We are also reviewing all relevant business practices regarding the security of Blackbaud data. We have been informed by Blackbaud that it has implemented numerous security changes. Specifically, Blackbaud stated that it quickly identified the vulnerability associated with this incident and took swift action to fix it. Blackbaud also stated that it has confirmed through testing by multiple third parties that its fix withstands all known attack tactics. Finally, Blackbaud has 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 public, we still recommend that you take precautions and have included some additional steps you can take to protect yourself as you deem appropriate.

For more information about this incident, you can consult the Blackbaud website at blackbaud.com/securityincident. If you have additional questions about this incident, please call 1-844-416-6281, toll-free, Monday through Friday, 8:00 a.m. to 5:00 p.m. ET. We apologize for any inconvenience this may have caused you.

Sincerely,

Michael Ehrhardt
Head of School

STEPS YOU CAN TAKE

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, Blackbaud is 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/epiq263?ac=263HQ1179

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.)

➢ **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 residents of North Carolina:** The North Carolina Office of the General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, and www.ncdoj.com. **For residents of Maryland**: The Maryland Office of the Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us. **For residents of New York**: The Attorney General may be contacted at: Office of Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/. **For residents of Rhode Island**: The Rhode Island Office of the Attorney General can be contacted at: 150 South Main Street, Providence, RI 02903, 1-401-274-4400, and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident. **For residents of Washington, D.C.**: The Attorney General may be contacted at: 400 6th Street NW, Washington, D.C. 20001; (202) 727-3400; and, https://oag.dc.gov/.

➢ **FILE OR OBTAIN A POLICE REPORT.** You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report incidents of identity theft to local law enforcement or to the Attorney General.

➢ **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.