August __, 2020

[Name]
[Address]
[City, State Zip]

Re: Notice of Data Breach

Dear [Name]:

We are writing to notify you that a national cyber incident with one of our vendors may have involved your personal information. As you may know, we, as well as many schools and nonprofits, rely upon the data management services of Blackbaud to support our fundraising and engagement efforts.

Because we highly value your relationship with Concord Academy, and because we take the privacy of your information very seriously, we are notifying you as a precautionary measure, to inform you and to explain steps that you can take to help protect your information.

What Happened

On July 16, 2020, Blackbaud notified us of a security incident and provided us with the following information:

Blackbaud recently discovered and stopped a ransomware attack. Prior to locking the cybercriminal out, the cybercriminal removed a copy of Blackbaud's backup file containing information maintained by many schools, colleges, universities, and non-profit organizations across the country, including Concord Academy. Blackbaud determined that the threat actor was in its computer network at some point beginning on February 7, 2020 and could have been present intermittently until May 20, 2020. After discovering the attack, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files, and ultimately expelled them from the system. Because protecting customers' data is their top priority, Blackbaud paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, Blackbaud 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.

As soon as we learned about this, we launched an investigation to understand what happened. We also engaged legal counsel with expertise in cyber law to assist with our investigation.

What Information Was Involved

Blackbaud notified Concord Academy of files impacted by ransomware. We then conducted an evaluation of the information in those files. From our review, we determined that the compromised files included your contact information, demographic data, and a history of your relationship with Concord Academy, including philanthropic giving. In addition, on July 28, 2020, we determined that, despite our established policy which requires redacting account information, the file contained a pdf of a personal check that you had made payable to Concord Academy. Blackbaud reported that the cybercriminal **did not** access credit card information because that information was not stored in the file, and did not access Social Security numbers because that information was encrypted.

What We Are Doing

We are notifying you so that you can take immediate action to protect yourself. Ensuring the safety of your data is of the utmost importance to us. We continue to actively monitor this situation and follow-up with Blackbaud to ensure that Concord Academy data is not at risk. Our internal team is focused on best in class practices that emphasize the protection and security of all data consistent with our policies and procedures.

As part of its ongoing efforts to help prevent something like this from happening in the future, Blackbaud reported that it has already implemented the following changes designed to protect your data: (1) confirming through testing by multiple third parties, including the appropriate platform vendors, that Blackbaud's fix withstands all known attack tactics; and (2) accelerating its efforts to further harden its environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

What You Can Do

To help protect your information we recommend that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.

For More Information

We understand that you may have questions about this incident that are not addressed in this letter. We are available to speak with you to assist you with questions regarding this incident and steps you can take to protect yourself. Again, we apologize for any inconvenience caused by this incident.

Sincerely,

Amy Fredericks
Chief Financial Officer
(978) 402-2263

Alice Roebuck
Director of Advancement and Engagement
(978) 402-2237

Rick Hardy
Head of School, Dresden Endowed Chair
(978) 402-2400

INFORMATION ABOUT WAYS TO PROTECT YOURSELF

You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the Federal Trade Commission ("FTC") by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261 or navigating online to www.consumer.ftc.gov/features/feature-0014-identity-theft. You can write to the FTC at Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Obtain Your Credit Report

You should monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed below. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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 below. Additional information is available at www.annualcreditreport.com.

Security Freeze

You may place a security freeze on your credit reports, free of 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. **Under federal law, you cannot be charged to place, lift, or remove a security freeze**.

You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax; Experian; and TransUnion. To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com https://www.equifax.com/personal/credit-report-services/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com https://www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com https://www.transunion.com/credit-freeze

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and proof of that address and any previous addresses for the past five years; (5) legible photocopy of a government issued ID card; (6) Social Security card, pay stub or W2; and (7) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

STATE SPECIFIC INFORMATION

DISTRICT OF COLUMBIA residents: You may also obtain information about preventing and avoiding identity theft from the D.C. Attorney General's Office. This office can be reached at:

Office of the Attorney General of the District of Columbia
Office of Consumer Protection
441 4th Street, NW
Washington, D.C. 20001
www.oag.dc.gov
1-202-727-3400

NEW YORK residents: You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State
Division of Consumer Protection
1-800-697-1220
http://www.dos.ny.gov/consumerprotection

New York Attorney General
1-800-771-7755
http://www.ag.ny.gov/home.html