

Matthew H. Meade, Esq.
(412) 566-6983
mmeade@eckertseamans.com

RECEIVED

AUG 24 2020

CONSUMER PROTECTION

August 21, 2020

VIA FIRST CLASS MAIL

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

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

This notice is provided on behalf of my client, Concord Academy, pursuant to N.H. Rev. Stat. §359-C:20(I)(b), following a vendor data breach that involved the personal information of eight (8) New Hampshire residents. The personal information included names, addresses and Social Security numbers. Concord Academy will provide written notice to the affected individuals later today, via U.S. mail. The notice includes instructions on how to activate a complimentary, two-year subscription for identify theft protection services from Experian, as well as general advice on how to protect one's identity and obtain free credit reports and security freezes. A copy of the notice letter is enclosed. Additional information on the incident is below.

Concord Academy is a private college preparatory school located in Concord, Massachusetts that contracts with a national vendor, Blackbaud, for data management services in connection with expense management and accounting. On July 16, 2020, Blackbaud notified Concord Academy, along with many other schools and nonprofits, of a ransomware attack that may have involved unauthorized acquisition of certain information maintained on behalf of Concord Academy, but which Blackbaud believed was "unlikely" to have triggered breach notification obligations. Nevertheless, Concord Academy conducted its own investigation to determine whether the incident would require notice to affected individuals and/or regulators.

According to Blackbaud, the unauthorized acquisition began on February 7, 2020 and may have continued intermittently until May 20, 2020. Although Blackbaud received confirmation from the cybercriminals that the acquired information was destroyed upon Blackbaud's payment of the ransom demand, Concord Academy undertook its own investigation into the matter. As a result of its investigation, on July 28, 2020, Concord Academy determined that eight (8) New Hampshire residents' personal information may have been involved in the Blackbaud incident.

As of the date of this letter, Concord Academy is not aware of any inappropriate use of the personal information involved. Concord Academy is continuing to actively monitor this situation

and follow-up with Blackbaud to ensure that Concord Academy data is not at risk. Concord Academy's 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 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.

Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,

Matthew H. Meade
Matthew H. Meade, Esq. *KBSI*

MHM/
Enclosure



August 21, 2020

«Vendor»
«Street»
«City», «State» «Zip»

Re: Notice of Data Breach

Dear «Vendor»:

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 for expense management and accounting purposes.

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 and a history of your relationship with Concord Academy as a vendor. In addition, on August 3, 2020, we determined that the file contained your Social Security number, which had been maintained for tax and payment purposes.

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. You should report any incidents of suspected identity theft to your local law enforcement and state Attorney General.

To protect you from potential misuse of your information, we are offering you a complimentary, two-year membership in Experian's® IdentityWorksSM Credit 3B. For more information on identity theft prevention and Experian's® IdentityWorksSM Credit 3B, including instructions on how to activate your membership, please see the additional information provided in 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

Amy Fredericks
Chief Financial Officer
(978) 402-2263

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.

For Maine, Maryland, and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

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

MARYLAND residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
Toll-free: 1-888-743-0023

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>

NORTH CAROLINA residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
Toll-free: 1-877-566-7226

RHODE ISLAND residents: You have the right to file and obtain a copy of a police report concerning any fraud or identity theft committed using your personal information. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
Toll-free: 1-401-274-4400

**ADDITIONAL DETAILS REGARDING YOUR 24-MONTH
EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:**

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by: November 16, 2020** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code: «Code»**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877.288.8057** by **November 16, 2020**. Be prepared to provide engagement number **DB22103** as proof of eligibility for the identity restoration services by Experian. A credit card is **not** required for enrollment in Experian IdentityWorks. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877.288.8057**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.