ECKERT SEAMANS
ATTORNEYS AT LAW

Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

TEL: 412 566 6000
FAX: 412 566 6099

Sandy B. Garfinkel, Esq.
(412) 566-6868
sgarfinkel@eckertseamans.com

November 3, 2020

VIA FIRST CLASS MAIL

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

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

This notice is provided on behalf of my client, Thayer Academy, pursuant to N.H. Rev. Stat. §359-C:20(I)(b), following a vendor data breach that involved the personal information of two (2) New Hampshire residents. The personal information included the individuals' name, address, phone number, and Social Security number. Thayer Academy will provide written notice to the affected individuals later today, via U.S. mail. A copy of the notice letter is enclosed. Additional information on the incident is below.

Thayer Academy is a private school located in Braintree, Massachusetts, that contracts with a national vendor, Blackbaud, for data management. On September 29, 2020, Blackbaud notified Thayer Academy that a ransomware attack may have resulted in unauthorized acquisition of certain information maintained on behalf of Thayer Academy. Thayer Academy immediately 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, Thayer Academy undertook its own investigation into the matter. As a result of its investigation, on October 5, 2020, Thayer Academy determined that New Hampshire residents' personal information may have been involved in the Blackbaud incident.

As of the date of this letter, Thayer Academy is not aware of any inappropriate use of the personal information involved. Thayer Academy is continuing to activity monitor this situation and follow-up with Blackbaud to ensure that Thayer Academy data is not at risk. Thayer Academy's internal team is focused on best in class practices that emphasize the protection and security of all data, consistent with its 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 that Blackbaud's "fix" withstands all known attack tactics; and (2) accelerating its efforts to further harden its environment through enhancements to access managements, network segmentation, and deployment of additional endpoint and network-based platforms.

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

Sincerely,

/s/ Sandy B. Garfinkel, Esq.

SBG/
Enclosure

Thayer Academy
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

November 3, 2020

Robert L Gottfried
115 Montclair Dr
West Hartford, CT 06107-1266

C-19

Re: Notice of Data Breach

Dear Robert L Gottfried:

We are writing regarding a recent incident that occurred at Blackbaud, a national vendor that provides data management services to many schools and nonprofits, including Thayer Academy, which may affect the security of your personal information. Because we highly value your relationship with Thayer Academy and 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, along with many other schools and nonprofits, of a ransomware attack that may have involved unauthorized acquisition of certain information (including data maintained on behalf of Thayer Academy) between February 7, 2020 and May 20, 2020. Despite Blackbaud's assurances that notifying individuals of a data breach was likely unnecessary, we conducted our own investigation into the matter and determined that notice was proper. Accordingly, on September 16, 2020, we provided notice to those individuals whose information may have been involved in the Blackbaud incident.

On September 29, 2020, Blackbaud notified us that additional files may have been compromised that Blackbaud did not originally identify as being involved in the incident. Upon learning of this, we immediately engaged legal counsel with expertise in cyber law to assist us in commencing a thorough investigation to determine what additional information could have been impacted by the incident.

What Information Was Involved
Once Blackbaud notified us of the incident and provided access to the compromised files, we evaluated each of the documents to find out what information was involved, who may have been affected, and where those people resided. As a result of our investigation, we discovered on October 5, 2020 that your personal information was involved in the Blackbaud incident. That information may have included your name, address, telephone number and Social Security number.

What We Are Doing
The confidentiality, privacy, and security of your information is of the utmost importance to us. We have security measures in place to protect the security of information entrusted to us and that we share with vendors. In addition to notifying you, as part of our ongoing commitment to the security of personal information, we continue to actively monitor this situation and follow-up with the vendor to ensure that Thayer Academy data is not at additional 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. We are also providing notice of this incident to appropriate government agencies, consistent with our compliance obligations and responsibilities.

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 their efforts to further harden their environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.

What You Can Do

At this time, we are not aware of any misuse of information arising from this incident. However, out of an abundance of caution, we are notifying you so you can take additional actions to help protect your information. We strongly encourage you to take the following preventative measures to help detect and mitigate any misuse of your information:

1. Activate your complimentary, two-year credit monitoring and identity theft membership in Experian's® IdentityWorks℠. This product provides you with identity monitoring services, including fraud detection and identity theft restoration. For more information on identity theft prevention and Experian's® IdentityWorks℠, including instructions on how to activate your membership, please see the additional information provided at the end of this letter.

2. 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.

3. Report any incidents of suspected identity theft to your local law enforcement and state Attorney General. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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 this incident may cause. We deeply value your relationship with Thayer Academy. Should you have further questions, please call the following toll-free phone number: 1-833-800-0020.

Sincerely,

Theresa Jay
Chief Information Officer
Thayer Academy

Sincerely,

Julaine McInnis
Chief Financial and Operating Officer
Thayer Academy

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

You also may request a security freeze be added to your credit report at Experian's online Freeze Center, www.experian.com/freeze/center.html, by phone at 1-888-EXPERIAN (1-888-397-3742), or by mail to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013. More information on a security freeze can be found below.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. 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 above. 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.

For Colorado residents: You may obtain one or more additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

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. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically, which can help spot and address problems quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above.

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 above. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. 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 any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) 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. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place, you will need it if you choose to lift the freeze. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Helpful Information

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

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 MEMBERSHIP:

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

- Ensure that you **enroll by**: **January 21, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code**: [redacted]

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 **January 21, 2021**. Be prepared to provide engagement number [redacted] 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.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related 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.