MCLANE MIDDLETON

CAMERON G. SHILLING
Direct Dial: (603) 628-1351
Email: cameron.shilling@mclane.com
Licensed in NH and MA

November 19, 2020

Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03302

Re: Data Security Breach

To whom it may concern,

McLane Middleton, P.A. represents Proctor Academy ("Proctor"), which is located at 204 Main Street, Andover, New Hampshire 03216. We are writing to inform you about a data security breach that affects 233 residents of New Hampshire.

What Happened: Blackbaud, Inc. ("Blackbaud") is a technology provider headquartered at 65 Fairchild Street, Charleston, South Carolina 29492. Proctor uses certain software and cloud services provided by Blackbaud to manage certain information about its students, parents, alumni, donors, and other members of the Proctor community.

On July 16, 2020, Blackbaud informed Proctor that it was the victim of a ransomware attack. According to Blackbaud's communications at that time, although the cybercriminals were unsuccessful in their attempts to encrypt Blackbaud's networks, they were able to export backup files for certain databases that Blackbaud maintains for numerous customers. One of many such compromised files was a backup of Proctor's ResearchPoint database. Also, according to Blackbaud's communications at that time, any personally identifiable information ("PII") in the exported backup files, including any social security number ("SSN"), was encrypted.

On September 29, 2020, Blackbaud informed Proctor and many other schools and non-profits that its forensic experts confirmed that other databases may have been affected by the breach, and that those databases contained unencrypted SSNs. Specifically, Blackbaud informed Proctor that Blackbaud had retained a database file for an application that Proctor no longer uses on Blackbaud's cloud, and that the file contains unencrypted SSNs.

Blackbaud paid a ransom in exchange for assurances that the criminals destroyed and had not sold the information that they obtained from Blackbaud. According to Blackbaud, such assurances would have included an assurance of destruction of the legacy database file for

assurances would have included an assurance of destruction of the legacy database file for Proctor that contained SSNs. Although Blackbaud has stated that it believes that the attackers actually did destroy the information without selling it, Blackbaud has also assured Proctor and its other customers that it is nonetheless monitoring the criminal network on the dark web to detect if the information was or is sold.

What Information Was Involved: According to Blackbaud, the breach involved a legacy database of Proctor that contains SSNs for 7 residents of Maryland. While there is no indication to date that this information has been used for fraudulent or unlawful purposes, Proctor has taken the following measures to address this matter.

What Proctor Is Doing: On November 6, 2020, Proctor sent the attached notice to affected individuals for whom it had contact information. As explained in the notice, Proctor is providing affected individuals with a free, two-year membership in an Experian identity theft and fraud prevention program. In addition, Proctor informed individuals how to implement a fraud alert and freeze or lock their credit accounts, and is providing them with a toll free telephone hotline and email to address questions and concerns.

Thank you for your attention to this matter. Please contact us if you have any questions or we can be of any assistance with this matter.

Very truly yours,

/s/ Cameron G. Shilling

Cameron G. Shilling

Enclosures

Dear name,

I am writing to update you about a breach at one of Proctor Academy's vendors that involved your Social Security Number (SSN). You may have received a notice from us in July about a breach that occurred at Blackbaud. At that time, Blackbaud informed Proctor and many other schools and non-profits that the breach was limited to certain databases and did not include any personally identifiable information (PII). However, Blackbaud recently updated its prior notification, informing us and many others that the breach affected additional databases and, in fact, did involve PII in the form of SSNs. We are writing to you because your SSN was included in the additional databases compromised in the Blackbaud breach.

What Happened:

On July 16, 2020, Blackbaud informed Proctor that it was the victim of a ransomware attack. According to Blackbaud's communications at that time, although the cybercriminals were unsuccessful in their attempts to encrypt Blackbaud's networks, they were able to export backup files for certain databases that Blackbaud maintains for numerous customers. One of many such compromised files was a backup of Proctor's ResearchPoint database. Also, according to Blackbaud's communications at that time, any PII in the exported backup files, including any SSNs, were encrypted and therefore not compromised.

On September 29, 2020, Blackbaud informed Proctor and many other schools and non-profits that Blackbaud's forensic experts have confirmed that other databases may have been affected by the ransomware breach, and that those additional databases contained unencrypted SSNs. Specifically, Blackbaud informed Proctor that Blackbaud had retained a database file for one of its software applications, an application that Proctor no longer accesses or uses on Blackbaud's network, and that the file contains SSNs.

As we communicated in our letter in July, Blackbaud and its team of forensic experts and law enforcement agents negotiated with the cybercriminals and paid a ransom in exchange for assurances that the criminals had destroyed and not sold the information that they had obtained from Blackbaud. According to Blackbaud, such assurances would have included an assurance of destruction of the legacy database file that contained SSNs. Although Blackbaud has stated that it believes that the attackers actually did destroy the information without selling it, Blackbaud has also assured Proctor and its other customers that it is nonetheless monitoring the criminal network on the dark web to detect if the information was or is sold.

What Information Was Involved:

The information about you in the legacy database file retained by Blackbaud included your Social Security Number.

What Should You Do:

Since the Blackbaud breach involved your SSN, you are being offered Experian identity and credit protection services, free of charge to you, for a period of 24 months from the date you enroll. To receive these services, you must enroll ***within 90 days*** from the date of this letter. To activate your free membership, please follow these steps:

- Visit this website: [redacted]
- Provide the following activation code: [redacted]
- Enroll ***within 90 days*** from the date of this letter

This service will include the following:

Proactive Fraud Assistance. Experian provides access during the service period to a fraud specialist who will work with enrollees on a one-on-one basis, answering any questions or concerns you may have. Proactive Fraud Assistance includes the following features:

- Assisted placement of fraud alerts
- A credit report from each of the three credit bureaus
- Assistance with reading and interpreting credit reports
- Removal from credit bureau marketing lists
- Answering questions individuals have about fraud
- Providing individuals with educational materials and email alerts

Identity Theft and Fraud Resolution. Services are provided for enrollees who fall victim to an identity theft as a result of the Blackbaud breach. This includes the following features:

- Access to a personal fraud specialist via a toll-free number
- Creation of a fraud victim affidavit
- Documents and phone calls for credit grantor notification and fraud removal
- Notification to government and private agencies
- Assistance with filing a law enforcement report
- Case file creation for insurance and law enforcement
- Assistance with placement of credit freezes
- Customer service support for individuals when enrolling in monitoring products
- Assistance with review of credit reports for possible fraud
- Access to educational information and threat alerts

Once registered, you can access the monitoring services by selecting the "Use Now" link to fully authenticate your identity and activate your services. Please ensure you enroll ***within 90 days*** from the date of this letter and take this step to receive your alerts.

If you have questions about this service, or need assistance with it, please contact Experian at (888) 682-5911. Please be prepared to provide activation code [redacted] as proof of eligibility for the services.

A credit card is not required for enrollment in this program. You can contact Experian immediately regarding any identity or credit issues, and have access to the foregoing features once you enroll in the program.

Proctor strongly encourages you to promptly use the foregoing information to enroll yourself in these identity and credit monitoring services.

What Can You Do:

Because the Blackbaud breach involved your SSN, other measures you could take to further protect yourself are as follows: (1) obtain your credit reports from www.annualcreditreport.com, inspect them for any potentially fraudulent activity, and notify the creditor if fraudulent; and (2) either implement a 90-day fraud alert, or freeze/lock your files with each of the three major credit bureaus. You are entitled at this time to inspect your credit reports, implement a fraud alert, and freeze/lock your credit without charge to you. If you would like to do so, the following is the contact information for the three major credit bureaus:

Equifax	Experian	TransUnion
866-349-5191	888-397-3742	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Blackbaud has stated that it is working with law enforcement authorities at the Federal Bureau of Investigation (FBI), thus, Blackbaud may have filed police reports. Under certain state and federal laws, you may have a right to obtain a copy of such reports. If you wish to do so, you should contact the FBI. If you experience identity or credit fraud or other crime as a result of the Blackbaud breach, you should contact the FBI or your state or local police.

What We Are Doing:

Proctor has retained its cyber security attorney to ensure that Blackbaud has implemented appropriate protections to ensure that such an event does not reoccur, and to determine whether Blackbaud otherwise has appropriate controls in place to safeguard the privacy and security of information about members of the Proctor community.

Proctor Academy values the privacy and safety of our community. We apologize for any concern that this Blackbaud breach causes, and are here to answer any questions you have about it. If you have questions, please contact us at communications@proctoracademy.org or 603-735-6715. Thank you for your support and involvement with our school.

Sincerely,

Mike Henriques, P'11, '15
Head of School