



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

November 16, 2020

Bruce A. Radke
312-463-6211
312-819-1910 Direct Fax
bradke@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of a Data Security Incident

Dear Attorney General MacDonald:

We represent the Storm King School (“SKS”) in connection with an incident involving a company called Blackbaud, Inc. (“Blackbaud”) that may have impacted the personal information of two (2) New Hampshire residents. SKS is reporting the incident pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While SKS is notifying you of this incident, SKS does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

SKS contracts with Blackbaud to store its donor, student, staff, and alumni information within Blackbaud’s self-hosted environment. Blackbaud recently notified SKS, as well as hundreds of other organizations that use its products, that Blackbaud was impacted by a ransomware event. According to Blackbaud, in May 2020, an unauthorized third party attempted to deploy ransomware within Blackbaud’s environment, and also exfiltrated some data out of Blackbaud’s systems between April 18, 2020, through May 17, 2020. Blackbaud initially told SKS that sensitive personal information in its systems was encrypted and could not have been accessed. However, on October 2, 2020, Blackbaud informed SKS that the person who gained access to Blackbaud’s network could have accessed files in which certain unencrypted personal information is stored, including, individuals’ full names, Social Security numbers, and bank account numbers, depending on the individual. SKS has since worked diligently to identify the individuals whose personal information was contained in the Blackbaud systems and potentially impacted by this incident. While SKS is not aware of any fraud or identity theft to any individual as a result

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Seattle Washington, D.C. Wilmington
Polsinelli PC, Polsinelli LLP in California

75471522.2



The Honorable Gordon MacDonald
Office of the Attorney General
November 16, 2020
Page 2

of this incident and cannot confirm if any personal information was actually obtained by an unauthorized party, SKS is notifying the potentially impacted New Hampshire residents.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

SKS has identified two (2) New Hampshire residents who may have been impacted by this incident. SKS mailed notification letters to the impacted individuals on November 16, 2020. Included in the notification was information on ways the individuals can protect themselves against potential fraud and identity theft, as well as a telephone number they can call if they have any questions regarding the incident. For individuals whose Social Security number was involved, SKS is offering, through Blackbaud, a complimentary two-year membership of credit monitoring and identity theft protection. SKS, has also established a confidential telephone inquiry line to assist the affected New Hampshire residents with any questions they may have regarding the incident. Enclosed is a copy of the notice that is being sent to the New Hampshire residents via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident from Blackbaud, SKS conducted a comprehensive search for any personal information stored in the Blackbaud system that may have been impacted by the incident. SKS is notifying impacted individuals, providing them with information on how they can protect themselves against fraudulent activity and identity theft, and, for certain individuals, offering two years of complimentary credit monitoring and identity theft protection. Finally, SKS is reviewing its relationship with Blackbaud and the technical controls in place for securing SKS's data in the Blackbaud system.

CONTACT INFORMATION

Please do not hesitate contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

A handwritten signature in cursive script that reads "Bruce A. Radke".

Bruce A. Radke

Enclosure

Storm King School
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



B-163

November 16, 2020

Dear [REDACTED]:

We are writing to advise you of a recent data security incident involving a company called Blackbaud, Inc. ("Blackbaud"). The Storm King School contracts with Blackbaud to store our donor, student, and alumni information within Blackbaud's self-hosted environment. **At this point, we have received no indication that any such information has been used for fraud or identity theft purposes.** Nonetheless, we are providing you with this notice because your personal information may have been affected by the incident.

Blackbaud recently notified us, as well as hundreds of other organizations that use its products, that it was impacted by a ransomware event. According to Blackbaud, in May 2020, an unauthorized third party attempted to deploy ransomware within Blackbaud's environment, and also exfiltrated some data out of Blackbaud's systems. On October 2, 2020, Blackbaud informed us that the person who gained access to Blackbaud's network could have accessed files in which your name or personal information is stored, including your Social Security number.

Upon receiving this information, we reviewed our internal records to identify who may have been affected. We have also worked with Blackbaud to obtain additional information about the nature of the event to determine the risk to your personal information. Again, although we are not aware of any instances of fraud or identity theft, we are offering through Blackbaud a complimentary two-year membership of Single Bureau Credit Monitoring through CyberScout, LLC ("CyberScout"). This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Single Bureau Credit Monitoring through CyberScout is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and Single Bureau Credit Monitoring through CyberScout, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter.**

We value the trust you place in us and take our responsibility to safeguard your personal information seriously. We apologize for any inconvenience or concern this incident might cause. We are committed to taking steps to help prevent this from happening again, including reviewing our relationship with Blackbaud and the technical controls they have in place for securing our data. For further assistance, please call 1-800-265-0860 from 8am to 5pm Eastern Time, Monday – Friday.

Sincerely,

A handwritten signature in cursive script that reads 'Jonathan W. R. Lamb'.

Jonathan W. R. Lamb
Head of School

We are 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, we are 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.

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=\[REDACTED\]](https://www.cyberscouthq.com/epiq263?ac=[REDACTED]).

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.

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).

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. 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.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

Rhode Island Residents: We believe that this incident affected two (2) Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

District of Columbia Residents: District of Columbia residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at 441 4th Street, NW, Washington, DC 20001, 202-727-3400, oag@dc.gov, <https://oag.dc.gov/>.