



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

RECEIVED

DEC 14 2020

CONSUMER PROTECTION

December 11, 2020

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

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

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

Re: Notification of Potential Data Security Incident

Dear Attorney General MacDonald:

We represent Foxcroft School (“Foxcroft”) in connection with an incident that that may have impacted the personal information of six (6) New Hampshire residents, and we provide this notice on behalf of Foxcroft 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 Foxcroft is notifying you of this incident, Foxcroft does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

On July 16, 2020, Foxcroft’s cloud service provider, Blackbaud Inc. (“Blackbaud”) notified Foxcroft that it was impacted by a ransomware event. According to Blackbaud, ransomware was deployed within its environment in May 2020, and certain data was exfiltrated out of its systems between April 18, 2020 and May 7, 2020. At the time, Blackbaud first reported the incident to Foxcroft in July, Blackbaud said that most of the exfiltrated data (including any data that might be considered sensitive) was encrypted and therefore not viewable by the unauthorized person even after it was exfiltrated. However, on September 29, 2020, Blackbaud alerted Foxcroft that in fact certain Social Security numbers that it had initially thought were encrypted when exfiltrated were actually unencrypted and therefore viewable by the unauthorized party. Upon learning this new information from Blackbaud, Foxcroft immediately began reviewing its internal records to identify

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



December 11, 2020

Page 2

who may have been affected. Foxcroft is not aware of any fraud or identity theft to any individual as a result of this incident but is notifying the potentially impacted residents.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

The incident may have impacted six (6) New Hampshire residents. Foxcroft mailed notification letters to these individuals on today, December 11, 2020. Enclosed is a sample of the notice that is being sent to the impacted residents via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Foxcroft worked to get additional information from Blackbaud about the incident and the potentially impacted information so that it could notify potentially impacted individuals. Foxcroft is also providing complimentary identity theft protection services to the impacted individual through Experian. Finally, Foxcroft is reviewing its relationship with Blackbaud and the technical controls in place for securing Foxcroft's data in the Blackbaud systems.

CONTACT INFORMATION

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

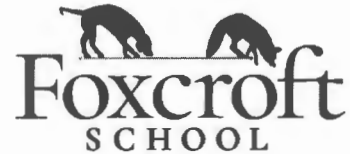
Very truly yours,

A handwritten signature in black ink, appearing to read "Bruce A. Radke".

Bruce A. Radke

Enclosure

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



[REDACTED]

December 11, 2020

Dear [REDACTED]:

Foxcroft School (“Foxcroft” or “we”) values and respects the privacy of your information, which is why we are writing this follow up notice to advise you of a recent incident that may have involved some of your personal information. We have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft. Nonetheless, we are writing to advise you of a recent security event involving a company called Blackbaud, Inc. (“Blackbaud”) that may have involved information about you.

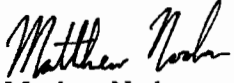
Over the years, Foxcroft, like many other schools, has contracted with Blackbaud to provide a variety of products that help us manage certain student, applicant, employee, and vendor data. As you may recall from our earlier communication about this breach, on July 16, 2020, Blackbaud notified us (as well as hundreds of other organizations that use its products) that it was impacted by a ransomware event. According to Blackbaud, ransomware was deployed within its environment in May 2020, and certain data was exfiltrated out of its systems between April 18, 2020 and May 7, 2020. At the time, Blackbaud first reported this to us in July, and to our relief, Blackbaud said that most of the exfiltrated data (including any data that might be considered sensitive) was encrypted and therefore not viewable by the unauthorized person even after it was exfiltrated.

On September 29, 2020, Blackbaud alerted us that its July report was incorrect. In this follow up notice, and to our frustration, Blackbaud explained that data it had initially thought was encrypted when exfiltrated was actually unencrypted and therefore viewable by the unauthorized party. This unencrypted data, Blackbaud reported, included certain individuals’ Social Security numbers, financial account numbers, and tax identification numbers. Upon learning this new information from Blackbaud, we immediately began reviewing our internal records to identify who may have been affected. Our review concluded that your name and bank account number were within the data set that the unauthorized person could have accessed.

While we are not aware of any fraudulent activity or misuse of any person’s information as a result of the incident, we are writing to alert you of what happened and to encourage you to diligently monitor your personal accounts. Additionally, in an abundance of caution, we are offering you a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. 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. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary membership, please see the additional information provided in this letter.**

We value the trust you place in us and apologize for any inconvenience or concern this incident might cause. Please know that we are taking steps to help prevent this from happening again, including reviewing our relationship with Blackbaud and the technical controls that it has in place for securing our data. If you need further assistance, please call 1-833-468-1010 from 8 a.m. to 5 p.m. Eastern Time, Monday – Friday.

Sincerely,

A handwritten signature in black ink that reads "Matthew Norko". The signature is written in a cursive style with a large initial 'M' and a stylized 'N'.

Matthew Norko
Director of Technology
Foxcroft School

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **March 7, 2021** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **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. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

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

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
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, 220 St. Paul Place, Baltimore, MD 21202, (888) 743-0023.

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, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226.

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 three (3) 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.

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).