

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

February 11, 2021

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Berwick Academy – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Berwick Academy. I am writing to provide notification of an incident at Blackbaud, Berwick Academy's third-party software and service provider, that may affect the security of personal information of approximately one thousand two hundred sixty-five (1,265) New Hampshire residents. Berwick Academy's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Berwick Academy does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On July 16, 2020, Blackbaud initially notified Berwick Academy of a security incident that impacted its clients across the world. Blackbaud reported to Berwick Academy that they identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed Berwick Academy that they stopped the ransomware attack and engaged forensic experts to assist in their internal investigation. That investigation concluded that the threat actor intermittently removed data from Blackbaud's systems between February 7, 2020 and May 20, 2020.

Once Berwick Academy was informed of the issue, Berwick Academy immediately initiated an internal investigation. As a part of its investigation, in addition to demanding detailed information from Blackbaud about the nature and scope of the incident, Berwick Academy engaged outside experts experienced in handling these types of incidents. On September 29, 2020, Blackbaud provided updated information to Berwick Academy. The update expanded the scope of the incident for Berwick Academy. Blackbaud identified instances where certain fields of sensitive personal information which Blackbaud initially assured Berwick Academy had been encrypted, were in fact not encrypted in certain fields of Blackbaud's database. On January 21, 2021, Berwick Academy determined that the information removed by the threat actor may have contained a limited amount of personal information, including full names and Social Security numbers.

February 11, 2021

Page 2

According to Blackbaud, they paid the threat actor to ensure that the data was permanently destroyed, and there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Blackbaud also indicates that it has hired a third-party team of experts, including a team of forensics accountants, to continue monitoring for any such activity. Nevertheless, out of an abundance of caution, Berwick Academy wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Berwick Academy is providing the affected residents with written notification of this incident commencing on or about February 10, 2021, in substantially the same form as the letter attached hereto. The affected residents are being offered complimentary two-year memberships with a credit monitoring service. Berwick Academy is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Berwick Academy, protecting the privacy of personal information is a top priority. Berwick Academy remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Blackbaud has assured Berwick Academy that they closed the vulnerability that allowed the incident and that they are enhancing their security controls and conducting ongoing efforts against incidents like this in the future. Berwick Academy continually evaluates and modifies its practices, and those of its third party service providers, to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

A handwritten signature in blue ink, appearing to read "Dominic A. Paluzzi".

Dominic A. Paluzzi

Encl.

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



[REDACTED]

[REDACTED]

[REDACTED]

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to Berwick Academy. We are writing with important information regarding a recent data security incident at Blackbaud, a third-party service provider, which may have involved some of the information that you provided to Berwick Academy. Blackbaud is a software and service provider that is widely used for accounting and academic purposes, as well as for fundraising and alumni or donor engagement efforts at non-profit organizations world-wide. Blackbaud experienced an incident impacting one or more of the applications used by Berwick Academy. We want to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On July 16, 2020, Blackbaud initially notified Berwick Academy of a security incident that impacted its clients across the world. Blackbaud reported to us that they identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed us that they stopped the ransomware attack and engaged forensic experts to assist in their internal investigation. That investigation concluded that the threat actor intermittently removed data from Blackbaud's systems between February 7, 2020 and May 20, 2020. According to Blackbaud, they paid the threat actor to ensure that the data was permanently destroyed. At that time, Blackbaud advised that personal information was encrypted and, therefore, not accessible to the threat actor.

On September 29, 2020 Blackbaud provided a second communication to Berwick Academy in which they identified instances where sensitive personal information that Blackbaud previously assured had been encrypted, was in fact not encrypted in Blackbaud's databases and potentially exposed to the threat actor.

What We Have Done.

Once we were informed of the issue, we immediately initiated an internal investigation. As a part of our investigation, in addition to demanding detailed information from Blackbaud about the nature and scope of the incident, we engaged outside experts experienced in handling these types of incidents to help determine the impact to our stakeholders and appropriately notify them.

What Information Was Involved.

On January 21, 2021, following an extensive review and analysis of the data at issue, we determined that the information removed by the threat actor may have contained some of your personal information, specifically your full name and Social Security number.

What You Can Do.

Based on the information Berwick has been provided, there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Blackbaud indicates that it has hired a third-party team of experts, including a team of forensics accountants, to continue monitoring for any such activity. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

Blackbaud is 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, a notification is sent to you the same day the change or update takes place with the bureau. In addition, Blackbaud is 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 to remediation support from a CyberScout Fraud Investigator. The enrollment instructions are included in this letter. For more information on identity theft prevention and these services, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures that you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis and report any suspicious activity to the proper authorities.

For More Information.

We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. Blackbaud has assured us that they closed the vulnerability that allowed the incident and that they are enhancing their security controls and conducting ongoing efforts against incidents like this in the future. We continually evaluate and modify our practices, and those of our third-party service providers, to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect your information. The response line is available Monday through Friday, 8am-5pm.

Sincerely,

[REDACTED]

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 24 month credit monitoring services, we recommend that you place an initial one (1) year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC

P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

PO Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-349-9960

Experian Security Freeze

PO Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016
<http://www.transunion.com/securityfreeze>
1-888-909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. 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.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

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 on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.