McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

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

April 6, 2021

VIA U.S. MAIL

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

Re: St. Johnsbury Academy – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents St. Johnsbury Academy. I am writing to provide notification of an incident at Blackbaud, St. Johnsbury Academy's third-party software and service provider, that may affect the security of personal information of approximately 72 New Hampshire residents. St. Johnsbury 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, St. Johnsbury Academy does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On July 16, 2020, Blackbaud notified St. Johnsbury Academy of a security incident that impacted its clients across the world. Blackbaud reported to St. Johnsbury Academy that they identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed St. Johnsbury 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. At that time, Blackbaud confirmed that the encryption level on encrypted fields was at least 256-bit encryption. Furthermore, Blackbaud also confirmed it had no evidence that the key (used to decrypt those protected fields) was compromised. Blackbaud later provided updated information to St. Johnsbury Academy. The update expanded the potential scope of the incident for St. Johnsbury Academy. According to its update, Blackbaud potentially identified instances where sensitive personal information which Blackbaud initially assured St. Johnsbury Academy had been encrypted, was in fact not encrypted in Blackbaud's databases.

Once St. Johnsbury Academy was informed of the issue, St. Johnsbury 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, St. Johnsbury Academy engaged outside experts experienced in handling these types of incidents to help determine the impact to its stakeholders and appropriately notify them. On March 29, 2021, following an extensive review and analysis of the data at issue, St. Johnsbury 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.

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, St. Johnsbury 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. St. Johnsbury Academy is providing the affected residents with written notification of this incident commencing on or about April 7, 2021, in substantially the same form as the letter attached hereto. St. Johnsbury Academy is offering the affected residents complimentary one-year memberships with a credit monitoring service. St. Johnsbury 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 St. Johnsbury Academy, protecting the privacy of personal information is a top priority. St. Johnsbury 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 St. Johnsbury 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. St. Johnsbury 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,

Dominic A. Paluzzi

Encl.

ST JOHNSBURY ACADEMY

[redacted]

Dear [redacted],

The privacy and security of the personal information we maintain is of the utmost importance to St. Johnsbury Academy. We are writing with important information regarding a recent data security incident at Blackbaud, Inc., a third-party service provider, which may have involved some of the information that you provided to St. Johnsbury Academy. Blackbaud is a software and service provider that is widely used for accounting, fundraising and alumni or donor engagement efforts at educational institutions and non-profits world-wide. Blackbaud recently experienced an incident impacting that application. 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 notified St. Johnsbury 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 confirmed that the encryption level on encrypted fields was at least 256-bit encryption. Furthermore, Blackbaud also confirmed it had no evidence that the key (used to decrypt those protected fields) was compromised.

Blackbaud later provided updated information to St. Johnsbury Academy. The update expanded the potential scope of the incident for St. Johnsbury Academy. According to its update, Blackbaud potentially identified instances where sensitive personal information which Blackbaud initially assured St. Johnsbury Academy had been encrypted, was in fact not encrypted in Blackbaud's databases.

What We Are Doing.

Upon learning of the issue, we commenced an immediate and thorough investigation. As part of our investigation, in addition to demanding detailed information from Blackbaud about the nature and scope of the incident, we engaged cybersecurity professionals experienced in handling these types of incidents.

What Information Was Involved.

On March 29, 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. Please know that we don't actively collect social security numbers, but this information may have been transferred from your original student application. If it existed, we have since removed that information from our alumni database.

What You Can Do.

According to Blackbaud, 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 continuing monitoring for any such activity. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

Furthermore, to protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorks℠ 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 one-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 against misuse of your information. The response line is available Monday through Friday, 8:00 am to 5:30 pm Central Time.

Sincerely,

St. Johnsbury Academy

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [redacted]
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 [redacted] 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.

2. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary 12-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.