

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

RECEIVED

FEB 08 2021

CONSUMER PROTECTION

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

P 1.248.646.5070
F 1.248.646.5075

February 3, 2021

VIA U.S. MAIL

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

Re: New Canaan Country School – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents New Canaan Country School. I am writing to provide notification of an incident at Blackbaud, a third party service provider, that may affect the security of personal information of two (2) New Hampshire residents. New Canaan Country School uses a Blackbaud application, and Blackbaud recently experienced an incident impacting that application. New Canaan Country School was one of many schools, colleges, and nonprofits that were a part of this incident. New Canaan Country School'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, New Canaan Country School does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On July 16, 2020, Blackbaud notified New Canaan Country School of a security incident affecting educational institutions and other nonprofits across the United States. Upon learning of the issue, New Canaan Country School commenced an investigation, which is still ongoing. Blackbaud reported to New Canaan Country School that Blackbaud identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed New Canaan Country School that they stopped the ransomware attack with the help of forensics experts and law enforcement, and that they prevented the cybercriminal from blocking or accessing encrypted files that contain sensitive data. Blackbaud engaged forensic experts to assist in their internal investigation. That investigation concluded that the cybercriminal removed data from Blackbaud's systems intermittently between February 7, 2020 and May 20, 2020. A backup file containing certain information was removed by the cybercriminal. According to Blackbaud, they paid the cybercriminal to ensure that the backup file was permanently destroyed. Upon learning of the issue, New Canaan Country School 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, New Canaan Country School engaged cybersecurity professionals experienced in handling these types of incidents.

Attorney General Gordon MacDonald
Office of the Attorney General
February 3, 2021
Page 2

On September 29, 2020, Blackbaud provided updated information to New Canaan Country School. The update expanded the scope of the incident for New Canaan Country School. Blackbaud identified instances where sensitive personal information which Blackbaud assured New Canaan Country School had been encrypted, was in fact not encrypted in Blackbaud's databases. Following an extensive review and analysis of the data file at issue, New Canaan Country School determined on January 5, 2021 that the information removed by the threat actor may have contained some of the residents' personal information. Specially, the data included the residents' names and tax identification numbers.

New Canaan Country School has no indication that any of the information has been misused. Nevertheless, out of an abundance of caution, New Canaan Country School 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. New Canaan Country School is providing the affected residents with written notification of this incident commencing on or about February 3, 2021 in substantially the same form as the letter attached hereto. The affected residents are being provided with 24 months of complimentary credit monitoring. New Canaan Country School 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 New Canaan Country School, protecting the privacy of personal information is a top priority. New Canaan Country School is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. New Canaan Country School continually evaluates and modifies its practices and internal controls 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.

Sincerely,



Dominic A. Paluzzi

Encl.

New Canaan Country School
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



**Important Information
Please Review Carefully**

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to New Canaan Country School. 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 New Canaan Country School. Blackbaud is a software and service provider that is widely used for accounting, fundraising and alumni or donor engagement efforts at non-profits and educational institutions 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 initially notified New Canaan Country School of a ransomware attack on their internal systems. Upon learning of the issue, we commenced an immediate and thorough investigation. As part of our investigation, we engaged external cybersecurity professionals experienced in handling these types of incidents.

Blackbaud reported to us that they identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud engaged forensic experts and law enforcement to assist in their internal investigation. The investigation concluded that the cybercriminal removed data from Blackbaud's systems intermittently between February 7, 2020 and May 20, 2020. A backup file containing certain information was removed by the cybercriminal. According to Blackbaud, they paid the cybercriminal to ensure that the backup file was permanently destroyed.

On September 29, 2020, Blackbaud provided updated information to New Canaan Country School. The update expanded the scope of the incident for New Canaan Country School. Blackbaud identified instances where sensitive personal information which Blackbaud assured New Canaan Country School had been encrypted, was in fact not encrypted in Blackbaud's databases.

What Blackbaud is Doing.

Blackbaud has stated that their teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. They indicate they have confirmed through testing by multiple third parties, including the appropriate platform vendors, that their fix withstands all known attack tactics. Additionally, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

What Information Was Involved.

On January 5, 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 [REDACTED].

What You Can Do.

According to Blackbaud, there is no evidence to support the belief 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.

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 by June 30, 2021. 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 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 5:00 PM Eastern Time.

Sincerely,

New Canaan Country School

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 24-Month Credit Monitoring.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please navigate to:

If prompted, please provide the following unique code to gain access to services:

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 by [REDACTED].

Proactive Fraud Assistance. 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.)

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. Consider 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.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-775 (TDD/TYY Support: 800-788-9898).

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.