Nutter

Seth Berman
Direct Line: (617) 439-2338
Fax: (617) 310-9338
E-mail: sberman@nutter.com

August 6, 2020
121437-1

Via FedEx

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

Re: Notice of Data Security Incident

Attorney General MacDonald:

My firm represents St. John's Preparatory School, an all-boys Catholic preparatory school for grades 6 through 12 located in Danvers, Massachusetts (St. John's Prep). Pursuant to N.H. Rev. Stat. § 359-C:20, I am writing to notify you of a data breach involving the personal information of twenty-five New Hampshire residents.

On Thursday, July 16, 2020, St. John's Prep was notified by Blackbaud Inc., a third-party software company that St. John's Prep and many other schools and non-profit organizations use as a database for advancement operations and financial accounting information, of a security breach involving accounts at Blackbaud. According to Blackbaud, in May 2020, Blackbaud discovered that cybercriminals had accessed their system and executed a ransomware attack. Blackbaud's investigation showed that the cybercriminals copied and exfiltrated certain data from Blackbaud's self-hosted environment before the hackers were locked out of the system. The hackers may have had access as early as February 7, 2020. Blackbaud has informed St John's Prep that its investigation showed that the cybercriminals were ultimately expelled from Blackbaud's system on or about May 20, 2020. We do not know why it took Blackbaud from May 20, 2020 until July 16, 2020 to inform us about the incident.

Blackbaud shared the following additional details regarding the data breach:

> In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access

> credit card information, bank account information, or social security numbers. Because protecting our customers' data was our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly.

Blackbaud informed St. John's Prep that a legacy St. John's Prep backup file from August 2019, stored by a Blackbaud vendor and kept according to Blackbaud policies, had been compromised. Blackbaud assured St. John's Prep that the database containing credit card, bank account, user names, passwords and social security numbers were encrypted, and thus that information could not have been accessed by the cybercriminals.

A few weeks before St. John's Prep was notified of the Blackbaud breach, it had discovered that a small subset of individuals had social security or credit card numbers that had been inadvertently entered into an unencrypted "Notes" field in its Blackbaud database. St. John's Prep deleted these inadvertent entries at that time. Once it learned of the Blackbaud breach, St. John's Prep determined from Blackbaud that the backup database that may have been accessed by the hackers predated St. John's Prep's attempt to remove the social security numbers and credit card numbers inadvertently stored in unencrypted fields in the database. Consequently, St. John's Prep is formally notifying and offering credit monitoring to those New Hampshire individuals whose social security numbers were in these unencrypted fields in the backup database exposed during the breach.

In addition to these twenty-five individuals in New Hampshire who we are formally notifying pursuant to N.H. Rev. Stat. § 359-C:20, there were approximately 1,920 additional New Hampshire individuals in the database whose data did not include personal information. While St. John's Prep is not required to provide formal notification to these individuals pursuant to N.H. Rev. Stat. § 359-C:20, in the interests of transparency and to keep its community informed of the incident, St. John's Prep did send an email to everyone in the database for whom they have email addresses informing them of the breach on July 23, 2020. For these individuals, the information potentially impacted by this incident may have included their contact information, demographic information, and information about their relationship with St. John's Prep.

St. John's Prep has been in communication with Blackbaud about its plan to ensure that nothing like this happens again. Blackbaud has informed St. John's Prep that it has taken actions to fix the vulnerability associated with the incident and confirmed through testing by multiple third parties, including the appropriate platform vendors, that the 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. Blackbaud also informed us that they worked with law enforcement in handling the incident.

As noted, above, St. John's Prep only learned about the incident on July 16, 2020. Once it learned of the incident, it moved as rapidly as possible to notify the affected people about the incident, first in an email that was sent to our entire community on July 23, 2020. We are notifying those individuals whose personal information was in the compromised August 2019 backup file by written notice today, on August 6, 2020. A copy of that notice is attached to this letter.

We deeply regret that this incident occurred and will be offering all individuals whose personal information was potentially released 24 months of complimentary identity protection services ID Experts's® MyIDCare™ service to help alleviate any concerns they may have resulting from this incident and to help prevent misuse of any information. As stated above, we have no evidence at this time of any fraud or misuse of any individual's information resulting from this incident.

Please do not hesitate to contact me if you have any questions.

Very truly yours,

Seth Berman

SPB2:jwg2
Enclosure

4891474.1

ST. JOHN'S PREP

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

August 6, 2020

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

At St. John's Preparatory School, we take the security of our community members' information very seriously, so it is out of an abundance of caution that we are informing you of an incident that occurred at a third-party software company that may have resulted in the disclosure of some of your personal information. We sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect your information and resources we are making available to you.

What Happened

On Thursday, July 16, 2020, St. John's Prep was notified of a security breach involving accounts at Blackbaud Inc., a third-party software company that St. John's Prep and many other schools and non-profit organizations use as a database for advancement operations and financial accounting information. In May 2020, Blackbaud discovered that cybercriminals had accessed their system and executed a ransomware attack. Blackbaud's investigation showed that the cybercriminals copied and exfiltrated certain data from Blackbaud's self-hosted environment before the hackers were locked out of the system. The hackers may have had access as early as February 7, 2020. Blackbaud has informed us that their investigation showed that the cybercriminals were ultimately expelled from their system on or about May 20, 2020. We do not know why it took Blackbaud from May 20, 2020 until July 16, 2020 to inform us about the incident.

Blackbaud shared the following additional details regarding the data breach:

> In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment.... Because protecting our customers' data was our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly.

What Information Was Involved

Blackbaud informed St. John's Prep that a legacy St. John's Prep backup file from August 2019, stored by a Blackbaud vendor and kept according to Blackbaud policies, was compromised. The potentially impacted information about you may have included your contact information, demographic information, and information about your relationship with St. John's Prep, including donation amounts and dates. You are receiving this letter because the compromised file also contained your social security number. **Please note that your credit card, bank account or other financial information was not involved in this incident.**

What We Are Doing

We are notifying you so that you can take immediate action to protect yourself. Ensuring the safety of your data is of the utmost importance to us. As part of their ongoing efforts to help prevent something like this from happening in the future, Blackbaud has assured us that they have already implemented several changes that are designed to protect your data from any subsequent incidents.

First, Blackbaud has informed us that they confirmed through testing by multiple third parties, including the appropriate platform vendors, that they have implemented fixes to their system designed to withstand all known attack tactics. Second, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms. And third, they have engaged a third-party team of experts to monitor the dark web for evidence of the exfiltrated data.

In order to ensure that you feel further protected from any potential impact, St. John's Prep is offering identity theft protection services through ID Experts® to provide you with MyIDCare™ services. MyIDCare services include 24 months of credit and CyberScan monitoring, $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

To receive credit monitoring you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What You Can Do

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities. To assist you in doing so we have attached a sheet of **Recommended Steps** that we recommend you consult.

We also encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday 9 am – 8 pm Eastern time. Please note the deadline to enroll is November 6, 2020.

For More Information

You will find detailed instructions for enrollment on the enclosed **Recommended Steps** document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-800-939-4170 or go to https://app.myidcare.com/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Edward B Hardiman

Edward Hardiman, Ph.D., P '19, '21, '26
Headmaster
St. John's Preparatory School

(Enclosure)

MyIDCare

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: 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 Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.
4883728.3