



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED
SEP 28 2020
CONSUMER PROTECTION

Angelina W. Freind
Office: (267) 930-4782
Fax: (267) 930-4771
Email: afreind@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

September 22, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Saint Joseph's College of Maine located at 278 Whites Bridge Rd, Standish, Maine, 04084, and are writing to notify your office of an incident that may affect the security of some personal information relating to two (2) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Saint Joseph's College of Maine does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about Thursday, July 16, 2020, Saint Joseph's College of Maine received notification from one of our third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Saint Joseph's College of Maine. Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud notified law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, Saint Joseph's College of Maine immediately commenced an investigation to determine what, if any, Saint Joseph's College of Maine data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On or about August 7, 2020, Saint Joseph's College of

Maine received further information from Blackbaud that allowed it to determine the scope of information potentially affected. On August 19, 2020, Saint Joseph's College of Maine's internal review of the impacted data set confirmed the exact constituent information that may have been subject to unauthorized access as a result of this event.

The New Hampshire resident information affected by this event includes name and financial account information.

Notice to New Hampshire Residents

On or about September 22, 2020, Saint Joseph's College of Maine provided written notice of this incident to affected individuals, which includes two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Saint Joseph's College of Maine moved quickly to investigate and respond to the incident, assess the security of Saint Joseph's College of Maine systems, and notify potentially affected individuals. Saint Joseph's College of Maine is also working to implement additional safeguards and training to its employees

Additionally, Saint Joseph's College of Maine is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Saint Joseph's College of Maine is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4782.

Very truly yours,



Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/eeb
Enclosure

EXHIBIT A



September 22, 2020

[Addressee]

[Street Address]

[City, State, Zip Code]

Dear [Salutation]:

We write to inform you of a recent incident that may affect the privacy of some of your information. On Thursday, July 16, 2020, we received notification from one of our third-party vendors, Blackbaud, Inc. (“Blackbaud”), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Saint Joseph’s College of Maine. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on our data. This notice provides information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

Blackbaud reports that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud notified law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. It is estimated that the breach occurred between May 14, 2020 to May 20, 2020. Upon learning of the Blackbaud incident, Saint Joseph’s College of Maine immediately commenced an investigation to determine what, if any, Saint Joseph’s College of Maine data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On or about August 7, 2020, Saint Joseph’s College of Maine received further information from Blackbaud that allowed it to determine the information potentially affected may have contained personal information.

Our investigation determined on or about August 19, 2020, that the involved Blackbaud systems contained your name and [impacted data elements]. Please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by the unknown actor. Blackbaud reports that no credit card information was included in the impacted files, and that no bank account information, usernames, passwords or Social Security numbers were accessible to the unauthorized actor as a result of this event.

The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures

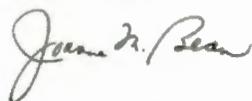
regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying regulatory authorities, as required.

We encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information.

We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (207) 893-7890 between the hours of 8:30 am - 4:30 pm, EST. You may also write to Saint Joseph's College of Maine at 278 Whites Bridge Rd, Standish, ME 04084.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

A handwritten signature in cursive script that reads "Joanne M. Bean".

Joanne M. Bean
Vice President & Chief Advancement Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Accounts

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

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

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For 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, and <https://ag.ny.gov/>.

For Rhode Island Residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this incident.