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

December 23, 2020

VIA U.S. MAIL

Office of Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188

Re: Bucknell University – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Bucknell University. 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 seven hundred and ten (710) Washington residents. Bucknell University uses a Blackbaud application, and Blackbaud recently experienced an incident impacting that application. Bucknell University was one of many schools, colleges, and nonprofits that were a part of this incident. Bucknell University'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, Bucknell University does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

On July 16, 2020, Blackbaud notified Bucknell University of a security incident affecting educational institutions and other nonprofits across the United States. Upon learning of the issue, Bucknell University commenced an investigation, which is still ongoing. Blackbaud reported to Bucknell University that Blackbaud identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed Bucknell University 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.

Bucknell University learned on December 2, 2020 that it is possible that the cybercriminal may have gained access to the Washington residents' names, dates of birth, mothers' maiden names and student identification numbers.

Bucknell University has no indication that any of the information has been misused. Nevertheless, out of an abundance of caution, Bucknell University 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. Bucknell University is providing the affected residents with written notification of this incident commencing on or about December 23, 2020 in substantially the same form as the letter attached hereto. Bucknell University 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 Bucknell University, protecting the privacy of personal information is a top priority. Bucknell University is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Bucknell University n 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.

Bucknell University
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

Bucknell
UNIVERSITY

[redacted]

NOTICE OF DATA BREACH

[redacted]

Dear [redacted]:

The privacy and security of the personal information we maintain is of the utmost importance to Bucknell University. 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 Bucknell University. Blackbaud is a software and service provider that is widely used for fundraising and alumni or donor engagement efforts at non-profits and universities world-wide. Bucknell University uses one or more Blackbaud applications, and Blackbaud recently experienced an incident impacting that application. We want to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

On July 16, 2020, Blackbaud notified Bucknell University 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.

What We Are Doing.

Upon learning of the issue, we commenced an immediate and thorough investigation. That investigation is still ongoing. 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 handing these types of incidents.

What Information Was Involved.

On December 2, 2020 we determined that the information removed by the threat actor may have contained some of your personal information, including your [redacted] **We have been assured that no information about Social Security numbers, bank accounts, passwords or credit or debit cards was compromised. Bucknell does not collect or store Social Security numbers nor credit card numbers, and online gifts are processed through a different system that was not involved in this incident.** Your demographic information, contact information, and/or philanthropic giving history, such as donation dates and amounts, may have been removed by the threat actor.

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 indicated that it has hired a third-party team of experts, including a team of forensic accountants, to continue monitoring for any such activity. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. This letter 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.

For questions regarding this incident, please contact [redacted]t at [redacted]u.

Sincerely,

[redacted]

Bucknell University

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

You may 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

2. 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 your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

3. 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.

4. 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.

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.