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

September 8, 2020

VIA U.S. MAIL

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

Re: University of Notre Dame – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents The University of Notre Dame. 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 three thousand two hundred nine (3,209) Washington residents. Notre Dame uses a Blackbaud software application as an engagement and fundraising service, and Blackbaud recently experienced an incident impacting that application. Notre Dame was one of many schools, colleges, and nonprofits that were a part of this incident. Notre Dame's notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Notre Dame does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

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

Notre Dame learned on August 11, 2020 that it is possible that the cybercriminal may have gained access to the Washington residents' names and dates of birth. The cybercriminal did not access financial account information, credit card account information or social security number information because Notre Dame does not maintain this information.

Notre Dame has no indication that any of the information has been misused. Nevertheless, out of an abundance of caution, Notre Dame 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. Notre provided the affected residents with written notification of this incident commencing during the week of August 28, 2020 in substantially the same form as the letter attached hereto. Notre Dame 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 Notre Dame, protecting the privacy of personal information is a top priority. Notre Dame is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Notre Dame 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.

UNIVERSITY OF NOTRE DAME

University Relations
405 Main Building
Notre Dame, Indiana 46556 USA

August 18, 2020

<<Mailing_Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<ZIP>>

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear <<First Name>>,

The privacy and security of the personal information we maintain is of the utmost importance to the University of Notre Dame. 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 the University of Notre Dame. 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. The University of Notre Dame 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 the University of Notre Dame 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, which is ongoing. As part of our investigation, we worked with Blackbaud to obtain detailed information about the nature and scope of the incident, and engaged cybersecurity professionals experienced in handling these types of incidents.

What Information Was Involved.

After Blackbaud's notification to Notre Dame, we have determined that the information removed by the threat actor may have contained some of your personal information, including your full name and date of birth. Your Social Security number, financial account information and/or payment card information were not exposed, as they were never provided to Blackbaud. Your demographic information, contact information, and/or philanthropic giving history, may have also 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 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. 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 the Office of Gift and Data Management at 574-631-5150.

Sincerely,

Lou Nanni
Vice President, University Relations
University of Notre Dame