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: Florida International University Foundation – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Florida International University Foundation ("FIU Foundation"). 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 nine hundred twenty-two (922) Washington residents. FIU Foundation uses a Blackbaud software application as an engagement and fundraising service, and Blackbaud recently experienced an incident impacting that application. FIU Foundation was one of many schools, colleges, and nonprofits that were a part of this incident. FIU Foundation's notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, FIU Foundation does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

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

FIU Foundation 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 FIU Foundation does not maintain this information.

FIU Foundation has no indication that any of the information has been misused. Nevertheless, out of an abundance of caution, FIU Foundation 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. FIU Foundation is providing the affected residents with written notification of this incident commencing on or about September 8, 2020 in substantially the same form as the letter attached hereto. FIU Foundation 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 FIU Foundation, protecting the privacy of personal information is a top priority. FIU Foundation is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. FIU Foundation 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.

Florida International University Foundation
[redacted]

413

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

September 8, 2020

Dear [redacted]:

At the FIU Foundation, there is nothing we value more than trust from our donors, alumni and our FIU community.

We are reaching out to you because the FIU Foundation has been notified by one of our third-party service providers, Blackbaud, about a recent ransomware attack. Blackbaud is a software solution that is widely used for fundraising and alumni or donor engagement efforts at non-profits, universities, healthcare organizations and foundations nationwide. Many organizations around the world have been impacted by this incident.

The FIU Foundation was notified on July 16, 2020 of the incident, which potentially has resulted in unauthorized access to certain information maintained on Blackbaud's software applications. Upon learning of this issue, we commenced an immediate and thorough investigation. The FIU Foundation uses Blackbaud to assist us in analyzing our fundraising efforts, and we only use Blackbaud to maintain publicly available information, such as constituent names, addresses and, in some cases, birthdates. This usage **does not** include Social Security numbers, credit card numbers or financial institution information.

On August 11, 2020, we determined that the information maintained on Blackbaud's software system may have contained some of your personal information, including your full name and date of birth. Again, **your Social Security number, financial account information and/or payment card information were not included.**

According to Blackbaud, there is no evidence to indicate that any data was or will be misused, disseminated, or otherwise made publicly available. Nonetheless, in light of this incident, we encourage you to be vigilant and protect yourself against spam or fraudulent emails or other communications seeking financial or related information. Additionally, 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. You always should 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.

Please be assured that we take the protection of your information very seriously. If you have any further questions regarding this incident, please contact our dedicated and confidential toll-free response line at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect your personal information. The response line is available Monday through Friday, 8 a.m. to 5 p.m. EST.

Thank you for your continued support of Florida International University and the FIU Foundation.

Respectfully,

[redacted]

[redacted] The FIU Foundation, Inc.

– 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.

FIRST CLASS MAIL

McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins LLC
600 Superior Avenue, East
Suite 2100
Cleveland, OH 44114

www.mcdonaldhopkins.com

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