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

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

July 12, 2019

VIA U.S. MAIL

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Hamilton College – Incident Notification

Dear Mr. Delaney:

McDonald Hopkins PLC represents Hamilton College ("Hamilton"). I am writing to provide notification of an incident at Hamilton that may affect the security of personal information of approximately one (1) New Hampshire resident. Hamilton's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission. By providing this notice, Hamilton does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Hamilton learned that an unauthorized individual obtained access to its admissions platform between March 2 and March 4, 2019. Upon learning of this issue, Hamilton began a prompt and thorough investigation, working very closely with law enforcement and external cybersecurity professionals. After an extensive forensic investigation and manual document review, Hamilton discovered on June 14, 2019 that the admissions platform that was accessed contained some of the resident's personal information. The information included the resident's health information and government-issued identification number.

Hamilton's investigation is ongoing. Nevertheless, out of an abundance of caution, Hamilton wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. Hamilton is providing the affected resident with written notification of this incident commencing on or about July 12, 2019 in substantially the same form as the letter attached hereto. Hamilton is advising the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Hamilton is advising the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Hamilton, safeguarding personal information is a top priority. Hamilton is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Hamilton is continuing to evaluate its practices and internal controls to enhance the security and privacy of personal information and will make changes, as necessary.

Should you have any questions regarding this notification, please contact me at (248)-220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,

James J. Giszczak

Encl.

Hamilton College
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

Hamilton

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

July 12, 2019

Dear [redacted]:

I am writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Hamilton College. As such, we wanted 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?

As we previously reported, we learned that an unauthorized individual obtained access to our admissions platform between March 2 and March 4, 2019.

What Are We Doing?

Upon learning of this issue, we began a prompt and thorough investigation. As part of our investigation, we have worked very closely with law enforcement and external cybersecurity professionals. After an extensive forensic investigation and manual document review, we discovered on June 14, 2019 that the admissions platform that was accessed contained some of your personal information.

As we previously noted, data such as credit card information and social security numbers that are associated with admission applications are encrypted in our data base and are therefore inaccessible to unauthorized individuals. However, in a small number of cases, supplemental application materials (such as transcripts or essays) might have included Social Security numbers, medical or health information, or other identifying information. The supplemental application materials containing your information were accessed.

What Information Was Involved?

The supplemental application materials in the accessed admissions platform contained some of your personal information, including your full name and medical or health information, and may have included your passport number, visa number, or other government-issued identification number.. Your Social Security number was **not** impacted.

What Can You Do?

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

This letter also provides other precautionary measures 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.

For More Information.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday 8:00 AM to 5:00 PM ET.

Sincerely,

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

You may place an initial 90-day "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

3. Consider 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.

4. 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.

5. 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.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: 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.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.