

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

March 15, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Carleton College – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Carleton College (“Carleton”) of Northfield, Minnesota. I am writing to provide notification of an incident that may affect the security of personal information of approximately one (1) Maryland resident. By providing this notice, Carleton does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Carleton recently experienced a phishing campaign that was directed to current students and faculty. As a result of this campaign, Carleton learned that an unauthorized individual gained access to multiple Carleton email accounts and online campus platforms. Upon learning of this issue, Carleton contained and secured the threat and commenced a prompt and thorough investigation. As part of its investigation, Carleton has been working very closely with external cybersecurity professionals experienced in handling these types of incidents.

Following a forensics investigation and internal review of the online platforms, Carleton discovered on March 1, 2024 that a page within one of its online platforms containing personal information was potentially accessed and/or viewed by an unauthorized party around December 18, 2023. The personal information pertaining to the Maryland resident included the individual’s passport number.

Carleton is providing the affected resident with written notification of this incident commencing on or about March 15, 2024, in substantially the same form as the letter attached hereto. Carleton will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. The affected resident will also be provided with the contact information for the consumer reporting agencies, the Maryland Attorney General, and the Federal Trade Commission.

At Carleton, protecting the privacy of personal information is a top priority. Carleton is committed to maintaining the privacy of personal and financial information in its possession and has taken many precautions to safeguard it.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,

A handwritten signature in blue ink, appearing to read "Dom Paluzzi", is positioned above the printed name.

Dominic A. Paluzzi

Encl.



One North College Street
Northfield, MN 55057



***IMPORTANT INFORMATION,
PLEASE REVIEW CAREFULLY***

March 15, 2024

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to Carleton College (“Carleton”). We are writing with important information regarding a security incident that may have involved your personal information. As such, 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?

Carleton recently experienced a phishing campaign that was directed to current students and faculty. As a result of this campaign, we learned that an unauthorized individual gained access to multiple Carleton email accounts and online campus platforms.

What We Are Doing.

Upon learning of this issue, we contained and secured the threat and commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents.

What Information Was Involved?

Following a forensics investigation and internal review of the online platforms, we discovered on March 1, 2024 that a page within one of our online platforms containing your [REDACTED] [REDACTED] was potentially accessed and/or viewed by an unauthorized party around December 18, 2023.

What You Can Do

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. This letter provides precautionary measures you can take to protect your personal information, including placing a fraud alert and security freeze on your credit files, and 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 are committed to maintain the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information, including updating passwords and enhancing email access protocols.

If you have any further questions regarding this incident, please reach out to [REDACTED] at [REDACTED] or [REDACTED]

Sincerely,

Carleton College

– OTHER IMPORTANT INFORMATION –

1. **Placing a Fraud Alert.**

You can place an initial one-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 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(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

P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(800) 349-9960
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(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 you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

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.

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.

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, <https://www.marylandattorneygeneral.gov/>, Telephone: 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.