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
jgiszczak@mcdonaldhopkins.com

April 10, 2017

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

Re: Connecticut College – Incident Notification

Dear Attorney General Delaney:

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

On January 20, 2017, an employee responded to an email by clicking a link within the message that compromised the email account. Connecticut College discovered the issue within minutes, and promptly changed the password. Since then, Connecticut College has closely monitored the account to ensure that no suspicious activity was taking place. In addition, Connecticut College immediately launched an investigation to analyze the extent of any compromise to the email account and the security of the emails and attachments contained within it. The investigation confirmed that an unauthorized third party had accessed the employee's email account over a very limited period of time. However, Connecticut College could not definitively conclude what information within the account, if any, was actually accessed, downloaded or acquired by the unauthorized user. The investigation confirmed the incident did not impact the security of any other email accounts, networks or servers.

After concluding the investigation on or about March 16, 2017, Connecticut College devoted considerable time and effort to determine what information, if any, was contained in the affected email account and, as such, may be at risk of disclosure. Based on the comprehensive investigation and document review, Connecticut College has confirmed that the compromised email account contained full name, address, date of birth, and may have included Social Security number or state ID/driver's license number.

To date, Connecticut College is not aware of any confirmed instances of identity fraud as a direct result of this incident. Nevertheless, Connecticut College wanted to make you (and the affected resident) aware of the incident and explain the steps Connecticut College is taking to help safeguard the resident against identity fraud. Connecticut College provided the New Hampshire resident with written notice of this incident commencing on April 5, 2017, in substantially the same form as the letter attached hereto. Connecticut College is offering the resident a complimentary membership with a credit monitoring and identity theft protection service. Connecticut College has advised the resident to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. Connecticut College has advised the resident about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The resident also has been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Connecticut College takes its obligation to help protect personal information very seriously. Connecticut College is continually evaluating and modifying its practices to enhance the security and privacy of personal information.

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

Sincerely,

James J. Giszczak

Encl.

CONNECTICUT COLLEGE

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

[redacted]

[redacted]

Dear [redacted],

I am writing to provide you with important details about a recent incident involving the security of your information and the measures we are taking to protect your information. On January 20, 2017, an employee responded to an email by clicking a link within the message that compromised the email account. We discovered the issue within minutes, and promptly changed the password. Since then, we have closely monitored the account to ensure that no suspicious activity was taking place. In addition, we immediately launched an investigation to analyze the extent of any compromise to the email account and the security of the emails and attachments contained within it.

The investigation confirmed that an unauthorized third party had accessed the employee's email account over a very limited period of time. However, we could not definitively conclude what information within the account, if any, was *actually* accessed, downloaded or acquired by the unauthorized user. The investigation confirmed the incident did not impact the security of any other email accounts, networks or servers.

After concluding the investigation, we devoted considerable time and effort to determine what information, if any, was contained in the affected email account and, as such, may be at risk of disclosure. Based on our comprehensive investigation and document review, we can confirm that the compromised email account contained your full name, address, date of birth, and may have included your Social Security number or state ID/driver's license number.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well.

To further protect you, we are providing you with a free, one-year membership to Experian's ProtectMyID® Alert, a credit monitoring and identity theft protection service. Enclosed in this letter, you will find enrollment information, as well as other precautionary measures you can take to protect your personal information, including placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity.

We take the security of personal information very seriously, and sincerely apologize for any inconvenience this incident may cause you. If you have questions, please do not hesitate to contact [redacted] at [redacted] or e-mail [redacted].

[redacted]

[redacted]

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Protecting your personal information is important to Connecticut College. In response to this security incident and as a precautionary measure, we have arranged for you to enroll in Experian's® ProtectMyID® Alert for a one year period at no cost to you. This protection is provided by Experian, one of the three major nationwide credit reporting companies.

Activate Experian's® ProtectMyID Now in Three Easy Steps:

1. ENSURE that you enroll by [redacted].
2. VISIT the ProtectMyID Web Site to enroll: [redacted]
3. PROVIDE your 9-character Activation Code: [redacted]

If you have questions or need an alternative to enrolling online, please call [redacted] and provide Engagement # [redacted].

Additional Details Regarding Your 12-Month ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after an incident. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance:** Immediately covers certain costs including lost wages, private investigator fees, and unauthorized electronic fund transfers. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.)

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted].

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you 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 <u>one</u> 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. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111
1-800-349-9960 (NY residents only)

Experian Security Freeze
P.O. 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

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 [redacted] or request your free credit reports online at [redacted]. 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.

6. Reporting Identity Fraud to the IRS.

If you believe that you are a victim of identity fraud and it is affecting your federal tax records (*or may affect* them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- **File an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf)**

- *Instructions for Form 14039* – In Section A check box 1. / In Section B check box 2. / Insert this in the "Please provide an explanation" box: My employer informed me that a third party unlawfully obtained an electronic file [W-2] containing certain employee personal information through a "phishing" scheme

- Call the IRS at (800) 908-4490, ext. 245 to report the situation (the unit office is open Monday through Friday from 7 am to 7 pm);
- Contact your tax preparer, if you have one; and/or
- You may call or visit your local law enforcement agency and file a police report. Please bring this notice with you.

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection

7. **Reporting Identity Fraud to the Social Security Administration.**

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

- The Social Security Administration has published Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf.