McDonald Hopkins
A business advisory and advocacy law firm®

600 Superior Avenue East
Suite 2100
Cleveland, OH 44114
P 216.348.5400
F 216.348.5474

Beth Gillin
Direct Dial: 216.348.5457
E-mail: bgillin@mcdonaldhopkins.com

August 31, 2024

VIA EMAIL: SecurityBreach@atg.wa.gov

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

Re: Connecticut College – Notification of Data Security Incident

To Whom It May Concern:

McDonald Hopkins PLC represents Connecticut College, located at 270 Mohegan Avenue in New London, Connecticut. I am writing to provide notification of an incident at Connecticut College that may affect the security of the personal information of at least seven hundred and eleven (711) Washington residents. By providing this notice, Connecticut College does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

Connecticut College determined that as a result of a data security incident, an unauthorized party accessed and acquired certain files maintained on Connecticut College's computer systems. Upon detecting the unauthorized activity on or about March 3, 2023, Connecticut College commenced an immediate and thorough investigation. As part of its investigation, Connecticut College engaged leading cybersecurity experts to identify what personal information, if any, might have been present in files accessed and/or acquired by the unauthorized party.

After an extensive forensic investigation and manual document review, Connecticut College preliminarily discovered on or about January 11, 2024 that one or more of the files accessed by the unauthorized party contained personal information pertaining to a limited number of individuals (including three hundred and five (305) Washington residents), such as full names, Social Security numbers, student identification numbers, education records information, financial aid information, taxpayer identification numbers, driver's license numbers, government-issued identification number(s), financial account information and/or access codes, health benefits/enrollment information, and medical record number and/or treatment information provided to Connecticut College Student Health Services. Not all information was included for all individuals.

Connecticut College provided the aforementioned affected individuals with written notification of this incident commencing on or about February 7, 2024. Connecticut College

offered the affected Washington residents complimentary one-year memberships with a credit monitoring service. Connecticut College advised 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 were also provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Connecticut College's investigation of the Incident, which concluded on or about July 15, 2024, determined that the Incident may affect the security of the personal information of an overall total of approximately seven hundred and eleven (711) Washington residents.[1] The four hundred and six (406) Washington residents who did not receive a notification letter in the first round of notification on or about February 7, 2024 were mailed a notification letter on or about August 7, 2024 in substantially similar form as the example attached at Exhibit A.

At Connecticut College, protecting the privacy of personal information is a top priority. Connecticut College is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Connecticut College continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

If you have any questions, please contact me at (216) 348-5457 or bgillin@mcdonaldhopkins.com.

Very truly yours,

BG/erb

Beth Gillin

[1] The 711 Washington residents includes the three hundred and five (305) Washington residents who were already sent a notification letter pertaining to this Incident on or about February 7, 2024.

EXHIBIT A

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

[redacted]

[redacted]

[redacted]

Dear [redacted]:

We are writing to inform you of a data security incident at Connecticut College involving some of your information. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

As a result of a data security incident, an unauthorized party accessed and acquired certain files maintained on our computer systems.

What We Are Doing.

Upon detecting the unauthorized activity on or about March 3, 2023, we promptly contained the incident and commenced a thorough investigation. As part of our investigation, we engaged leading cybersecurity experts to identify what personal information, if any, was involved.

What Information Was Involved?

After an extensive investigation and manual document review, which concluded on or about July 15, 2024, we determined that one or more of the files accessed and/or acquired by the unauthorized party contained your [redacted].

What You Can Do.

We have no evidence of any identity theft or financial fraud directly resulting from this incident. Out of an abundance of caution to protect you from potential misuse of your information, we are offering complimentary access to Experian IdentityWorks^{SM} Credit 3B for [redacted] months. For more information on identity theft prevention and Experian IdentityWorks^{SM}, including instructions on how to activate your complimentary [redacted]- month membership, please see the additional information provided in this letter.

This letter also provides other 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. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information on the following pages.

For More Information.

Please accept our apologies that this incident occurred. We are 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 and internal controls 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, 9:00 AM to 9:00 PM Eastern Time.

Sincerely,

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12 months Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** [redacted] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [redacted]
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by [redacted]. Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE[TM]:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 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/ce nter.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

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 cost. 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 30348-5788
https://www.equifax.com/personal/credit- report-services/credit-freeze/
(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.

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. Protecting Your Medical Information.

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.

6. 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.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

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.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 1-877-566-7226.

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

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828