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

Christine Czuprynski
Direct Dial: 248-220-1360
E-mail: cczuprynski@mcdonaldhopkins.com

RECEIVED
MAY 11 2020
CONSUMER PROTECTION

May 5, 2020

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Cincinnati State Technical and Community College – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Cincinnati State Technical and Community College ("Cincinnati State"). I am writing to provide notification of an incident at Cincinnati State that may affect the security of personal information of approximately two (2) New Hampshire residents. Cincinnati State's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Cincinnati State does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Cincinnati State recently learned that a limited number of employee email accounts were compromised by an email phishing attack resulting in unauthorized access to the email boxes. Upon learning of the issue, Cincinnati State immediately commenced a prompt and thorough investigation. As part of its investigation, Cincinnati State has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and reconstruction of the email boxes' content, Cincinnati State discovered on April 6, 2020 that the impacted email accounts that were accessed between October 2019 and January 2020 contained a limited amount of personal information, including the affected residents' full names, Social Security numbers, driver's license numbers and/or state identification numbers, bank account information, and credit or debit card information.

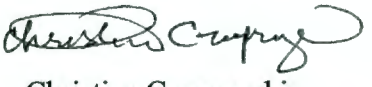
To date, Cincinnati State has no evidence that the contents of the mailboxes were reviewed, or that any of the information has been misused. Nevertheless, out of an abundance of caution, Cincinnati State wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Cincinnati State will provide the affected residents with written notification of this incident commencing on or about May 5, 2020 in substantially the same form as the letter attached hereto. Cincinnati State will offer the affected residents a complimentary one-year membership with a credit monitoring service. Cincinnati State will advise 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 will be advised to contact their financial institutions to inquire about steps to take to protect their accounts. The affected residents will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

Should you have any questions concerning this notification, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



Christine Czuprynski

Encl.

Cincinnati State
TECHNICAL AND COMMUNITY COLLEGE

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

Dear [redacted]

We are 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 Cincinnati State Technical and Community College ("Cincinnati State"). As such, 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?

We recently learned that a limited number of Cincinnati State employee email accounts were compromised by an email phishing attack resulting in unauthorized access to the email boxes.

What We Are Doing.

Upon learning of the issue, we immediately 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. After an extensive forensic investigation and reconstruction of the email boxes' content, we discovered on April 6, 2020 that the impacted email accounts that were accessed between October 2019 and January 2020 contained some of your personal information. We have no evidence that the contents of the mailboxes were reviewed, or that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

The impacted email accounts that were accessed contained archived documents with your personal information, specifically your full name, Social Security number, driver's license number and/or state identification number, bank account information, and credit or debit card information.

What You Can Do.

To protect you from potential misuse of your information, we are offering a complimentary one-year membership in Equifax® Credit Watch™ Gold. Equifax® Credit Watch™ Gold is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and Equifax® Credit Watch™ Gold, including instructions on how to activate your complimentary one-year 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/or security freeze on your credit files, and/or obtaining a free credit report. Because your bank account information and credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number. Additionally, you should always remain vigilant in reviewing your account statements for fraudulent or irregular activity on a regular basis.

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 a.m. to 9 p.m. Eastern Time.

Sincerely,

Cincinnati State Technical and Community College

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

[redacted]

Equifax® Credit Watch™ Gold provides you with the following key features:

- Equifax® credit file monitoring with alerts to key changes to your Equifax Credit Report
- Automatic Fraud Alerts[1] – With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit
- Wireless alerts (available online only) – Data charges may apply.
- Access to your Equifax® credit report
- Up to $25,000 Identity Theft Insurance[2]
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instructions

To sign up online for online delivery go to [redacted]

1. **Welcome Page:** Enter the Activation Code provided at the top of this page and click the "Submit" button.
2. **Register**: Complete the form with your contact information (name, gender, home address, date of birth, Social Security number and telephone number) and click the "Continue" button.
3. **Create Account:** Complete the form with your email address, create a Username and Password, check the box to accept the Terms of Use and click the "Continue" button.
4. **Verify ID**: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. **Order Confirmation:** This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

To sign up for US Mail delivery, dial 1 [redacted] **for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.**

1. **Activation Code:** You will be asked to enter your Activation Code as provided above.
2. **Customer Information:** You will be asked to enter your home telephone number, home address, name, date of birth and Social Security number.
3. **Permissible Purpose**: You will be asked to provide Equifax with your permission to access your Equifax credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. **Order Confirmation**: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

[1] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[2] Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. 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.

Equifax® is a registered trademark of Equifax Inc. ©2017 Equifax Inc., Atlanta, Georgia. All rights reserved.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 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	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

3. 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 sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	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 monitoring 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.

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. 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.