

Colin M. Battersby
Direct Dial: (248) 593-2952
E-mail: cbattersby@mcdonaldhopkins.com

March 22, 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: Lewis and Clark College – Incident Notification

To Whom it May Concern:

McDonald Hopkins PLC represents Lewis and Clark College (“Lewis and Clark”), located at 615 South Palatine Hill Road, Portland, Oregon 97219, regarding a recent security incident. I am writing to provide notification of an incident at Lewis and Clark that may affect the security of personal information of approximately two hundred and eighty (280) Maryland residents. Lewis and Clark will supplement this notification with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Lewis and Clark does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about March 3, 2023, Lewis and Clark became aware of potentially unauthorized access to their network due to a ransomware cybersecurity incident. Upon learning of this issue, Lewis and Clark immediately contained the threat by disabling all unauthorized access to the network and commenced a prompt and thorough investigation. Lewis and Clark also reported the incident to the Federal Bureau of Investigations and communicated with the Oregon Attorney General regarding the incident. As part of the investigation, Lewis and Clark has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Lewis and Clark kept its community apprised of relevant developments. Although at the time Lewis and Clark did not have evidence that personal data was accessed or acquired by an unauthorized individual, out of an abundance of caution, shortly following the incident Lewis and Clark offered employees and students access to complimentary credit monitoring services in the event the individuals were concerned that their information may have been impacted.

Unfortunately, the forensic investigatory team determined that the unauthorized party potentially accessed or removed data from the Lewis and Clark environment, specifically on portions of the file servers. Subsequently, Lewis and Clark conducted a thorough and detailed manual review of all the data contained on the impacted servers. Unfortunately, because the affected data was maintained within a file server, the review and analysis of the impacted data was painstaking and time-consuming. The affected system is a storage drive, not a searchable database, thus the unstructured nature of the data set necessitated a document-by-document review process.

At the completion of the review, Lewis and Clark determined on February 24, 2024, that personal information attributable to certain individuals was maintained on the servers and potentially may have been accessed or acquired by the unauthorized party. The information that may have been accessed or acquired may include name, Social Security number, driver's license or state identification, passport, financial account information, health insurance information, and/or medical information. Not all information was affected for all individuals. On March 19, Lewis and Clark located the most recent address of the impacted individuals. Lewis and Clark proceeded to promptly notify all potentially impacted individuals as expeditiously as possible and providing written notice on or about March 22, 2024. Lewis and Clark is also providing notice of the incident on its website and notifying major credit reporting agencies.

As stated above, upon learning of this issue, Lewis and Clark immediately commenced an internal investigation and promptly notified potentially affected individuals. Lewis and Clark has no evidence that the impacted information has been used to commit financial fraud or identity theft. Lewis and Clark 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. Lewis and Clark is offering residents with Social Security numbers impacted with a complimentary membership with a credit monitoring service. Lewis and Clark will advise the affected residents regarding precautionary measures to best protect their identity and financial accounts including: remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis; the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports; and contact information for the consumer reporting agencies and the Federal Trade Commission. The affected residents are also being provided with the contact information for the Attorney General for Maryland. A sample of the notice letter is included herein for your reference.

At Lewis and Clark, protecting the privacy of personal information is a top priority. Lewis and Clark is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Further, Lewis and Clark continues to evaluate and improve, where appropriate, its administrative and technical safeguards including training its employees on best practices related to cybersecurity, policies, procedures, and protocols, and tools to protect its network environment.

If you have any additional questions, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com.

Very truly yours,



Colin M. Battersby

Encl.



March 22, 2024

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to Lewis and Clark College. We are writing to provide you with information regarding a cybersecurity incident that potentially involved your personal information. Please read this notice carefully, as it provides information about the incident, the complimentary identity monitoring services we are making available to you, and the significant measures we take to protect your information.

What Happened?

On March 3, 2023, Lewis & Clark College detected unauthorized access to our network as a result of a cybersecurity incident that resulted in the exposure of certain data we maintain.

What We Are Doing.

Upon learning of the incident, we immediately took steps to secure our network and launched an investigation assisted by external cybersecurity professionals experienced in handling these types of incidents. Our investigation determined that the bad actors took data from our network environment on or about February 28, 2023. As such, we conducted an extensive manual review of the data residing on the impacted servers. On February 24, 2024, we determined that the impacted files contained your personal information.

While cybersecurity threats continue to impact all of us, we are taking ever-increasing measures to protect the information entrusted to us. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. In response to this incident and through our continuing comprehensive review, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts.

What Information Was Involved?

The exposed information contained your [REDACTED].

What You Can Do.

Although there is no evidence directly linking this incident to specific incidents of financial fraud or identity theft, we want to make you aware of the incident and to provide complimentary credit monitoring services as a precaution. We are providing you with access to complimentary identity theft protection services to further protect your information. We are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for [REDACTED] from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

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.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information.

If you have questions, please contact our dedicated and confidential call center at [REDACTED]. The response line is available for 90 days from the date of this letter, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. We apologize for any inconvenience or concern this may cause. We have taken this matter very seriously and will continue to take significant measures to protect the personal information in our possession.

Sincerely,
Lewis & Clark College

- OTHER IMPORTANT INFORMATION -

1. Placing a Fraud Alert.

We recommend that you place a 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
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(888) 378-4329

Experian

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

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
www.transunion.com/fraud-alerts
(800) 680-7289

2. 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
www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze-center.html
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
(888) 916-8800

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. 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 a credit monitoring service, 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. Protecting Your Medical Information.

If this notice letter indicates that your medical information was impacted, we have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from 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.

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.

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, www.marylandattorneygeneral.gov, Telephone: 888-743-0023. **Massachusetts Residents:** Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. **New Mexico residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit. In addition, you have the right to obtain a security freeze (as explained above) or submit a declaration of removal. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act. For more information about the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. **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; 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: 877-566-7226 (Toll-free within North Carolina), 919-716-6000. **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. **Rhode Island Residents:** You have the right to obtain a police report if one was filed, or alternatively, you can file a police report. Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above. In order to request a security freeze, you may need to provide the following information: your full name (including middle initial as well as Jr., Sr., II, III, etc.); Social Security number; date of birth; complete address; prior addresses; proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.); and if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. When you place a security freeze on your credit report, within five (5) business days you will be provided with a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following: (1) the unique personal identification number or password provided by the consumer reporting agency; (2) proper identification to verify your identity; and (3) the proper information regarding the period of time for which the report shall be available to users of the credit report. There were 25 Rhode Island residents impacted. **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, oag.dc.gov/consumer-protection, Telephone: 202-442-9828.