

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

December 6, 2023

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

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

Re: Jersey College – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents Jersey College. I am writing to provide notification of an incident at Jersey College that may affect the security of personal information of approximately fifty-five (55) Maryland residents. By providing this notice, Jersey College does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On January 25, 2023, Jersey College detected unauthorized access to its network due to a network security incident. Jersey College immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations. Based on its comprehensive investigation, Jersey College determined that an unauthorized party potentially accessed and removed files from the network between January 11, 2023, and January 25, 2023.

Upon completion of the investigation, Jersey College began a comprehensive manual review of the impacted files. On November 29, 2023, Jersey College discovered that personal information was removed from its network in connection with this incident, including the affected residents' full names or first initials with last names and or more of the following: date of birth, bank account and routing number, payment card information, citizenship registration number, Social Security number, driver's license, government issued identification number, student identification number, passport number, visa number, account access credentials, medical information, and health insurance information. Not all information was impacted for all individuals.

To date, Jersey College is not aware of any reports of identity theft or financial fraud as a direct result of this incident. Nevertheless, out of an abundance of caution, Jersey College wanted

to inform you (and the affected residents) of the incident and explain the steps that it is taking to help safeguard the affected residents against identity fraud. Jersey College is providing the affected residents with written notification of this incident commencing on or about December 5, 2023 in substantially the same form as the letter attached hereto as **Exhibit A**. Jersey College is offering the affected residents whose Social Security numbers were impacted complimentary one-year memberships with a credit monitoring service. Jersey College is advising 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 are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission. The affected residents are also being provided steps to take to safeguard themselves against medical identity theft.

To prevent a similar event from occurring in the future, Jersey College has implemented new, and upgraded existing, technical safeguards to improve its cybersecurity posture. For example, Jersey College improved its network monitoring and threat detection and prevention solutions and protocols; further restricted user access to in accordance with the principle of least privilege, and upgraded and/or patched hardware and software systems. Jersey College implemented additional cybersecurity training for users and hired additional employees in the IT Department.

At Jersey College, protecting the privacy of personal information is a top priority. Jersey College is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Jersey College 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) 593-2952 or cbattersby@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



Colin M. Battersby

Encl.

Exhibit A



P.O. Box 989728
West Sacramento, CA 95798-9728



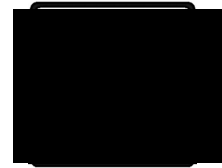
43-008769



008769

Enrollment Code: [REDACTED]

To Enroll, Scan the QR Code Below:



Or Visit:



December 5, 2023

***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

Dear [REDACTED]

We are writing with important information regarding a recent data security incident. The privacy and security of the personal information we maintain is of the utmost importance to Jersey College. We want 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 personal information.

What Happened?

On January 25, 2023, Jersey College experienced unauthorized access to our network due to a cybersecurity incident.

What We Are Doing.

Upon learning of this issue, we commenced a prompt and thorough investigation in consultation with external cybersecurity professionals who regularly investigate and analyze these types of incidents. Based on the comprehensive investigation and manual document review, we determined on November 29, 2023 that an unauthorized party potentially accessed and removed files containing your personal information from our network between January 11, 2023, and January 25, 2023.

What Information Was Involved?

The impacted files contained your full name and **Date Of Birth, Social Security Number.**

What You Can Do.

We have no evidence of financial fraud or identity theft related to this data. Out of an abundance of caution, and to protect you from potential misuse of your information, we are offering **complimentary** identity theft protection services through IDX, A ZeroFox Company, the data breach recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on identity theft prevention and IDX identity protection services including instructions on how to activate your complimentary 12-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, explanation of benefits 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 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 1-██████████ 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 am – 9 pm Eastern Time.

Sincerely,

Jersey College
546 US Highway 46
Teterboro, NJ 07608
201-645-██████



– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring

Go to [REDACTED] follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Please note that the enrollment deadline is March 5, 2024. Note: You must have established credit to use the credit monitoring service. If you need assistance, IDX will be able to assist you.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial one (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

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

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 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 30348-5788
<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 will 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 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 twelve (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.

If this notice letter states that your financial account information and/or 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.

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.

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: 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.

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.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.



The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided 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.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

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:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. 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.

There were 6 Rhode Island residents impacted by this incident.

