

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

March 3, 2025

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: Loyola University Maryland – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents Loyola University Maryland (“Loyola”) located at 4501 N Charles St., Baltimore, Maryland 21210. I am writing to provide notification of a security incident that impacted Loyola and may affect the security of personal information of approximately six (6) Maryland residents.

On or around July 25, 2024, Loyola identified a potential cybersecurity incident involving one (1) corporate email account. Upon learning of this issue, Loyola immediately commenced a prompt and thorough investigation. As part of its investigation, Loyola worked very closely with external cybersecurity professionals experienced in handling these types of incidents. Following a forensics investigation and complex manual document review, Loyola discovered on January 30, 2025, that the files in the impacted account that were potentially access or acquired by the unauthorized third-party actor between July 19, 2024 and July 25, 2024 contained residents’ personal information, including full name, Social Security number / individual tax identification number, government identification, financial account number(s), medical information and health insurance information.

Loyola is not aware of any reports of identity fraud or improper use of personal information as a direct result of this incident. Nevertheless, out of an abundance of caution, Loyola wanted to inform you (and affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. Loyola is providing the affected residents with written notification of this incident, commencing on or about February 28, 2025 in substantially the same form as the letter attached hereto. Loyola is offering the affected residents complimentary one-year memberships with a credit monitoring service, for those with Social Security number involved. Loyola is also advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports.

March 3, 2025

Page 2

The affected residents are also being provided with the contact information for the consumer reporting agencies, the Federal Trade Commission, and the Maryland Attorney General.

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

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,



Dominic A. Paluzzi

Encl.



LOYOLA
UNIVERSITY MARYLAND

4501 N Charles St.
Baltimore, MD 21210

February 28, 2025

[REDACTED]
[REDACTED]
[REDACTED]

***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

Dear [REDACTED]

The privacy and security of the personal information we maintain is important to Loyola University Maryland ("Loyola"). We are writing with important information regarding a data security incident that involved your personal information. 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 information.

What Happened?

On or about July 25, 2024, Loyola experienced a security incident impacting one (1) university email account.

What We Are Doing.

Upon learning of this 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. Following a forensics investigation and complex manual document review, we discovered on January 30, 2025, that the files in the impacted account that may have been accessed or acquired by the unauthorized actor between July 19, 2024 and July 25, 2024 contain your personal information.

What Information Was Involved?

The at-risk files contained some of your personal information, including your full name, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

What You Can Do.

We have no evidence that any of your information has been misused as a direct result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the scope of the incident and offer a **complimentary 12-month membership** of identity theft protection services through IDX, A ZeroFox Company. IDX identity protection services include: **12-month membership** 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.

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 on a regular basis and report any fraudulent or irregular activity immediately. The enclosed “Other Important Information” provides further details regarding what you can do.

For More Information

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 or email us at [REDACTED] or [REDACTED], Monday through Friday, 8:00 a.m. to 3:00 p.m. Eastern Time, excluding holidays.

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.

Sincerely,

Loyola University Maryland

OTHER IMPORTANT INFORMATION

1. Enrolling in Complimentary Credit Monitoring.

- **Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code: [REDACTED]
- **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. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- **Telephone.** Contact IDX at **1-800-939-4170** to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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-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. 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
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(800) 349-9960
(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. Please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

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.

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.

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.

Consider keeping a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is helpful to log conversations with creditors, law enforcement officials, and other relevant parties.

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.