

January 8, 2024

BY EMAIL

Idtheft@oag.state.md.us

Office of the Attorney General
State of Maryland
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notification Pursuant to M.C. § 14-3504(h)

To the Office of Attorney General:

Pursuant to the above statute, Loyola University of Chicago (“Loyola”), hereby submits this notice of an information security incident. In approximately December 2021, an unknown individual obtained unauthorized access to personal information of Loyola student-athletes maintained on the system of Athletic Trainer Systems (“ATS”), a third party vendor. ATS first reported this unauthorized access to Loyola in November 2023 in the attached letters. The incident impacted three (3) Maryland residents. To date, Loyola has no information that such personal information was actually used.

Enhanced password requirements were instituted in 2021 by the vendor to prevent a recurrence of such an incident. Loyola continues to investigate the incident in order to institute additional safeguards to prevent any recurrence. Loyola is taking steps to further increase information security awareness training as well as identifying technology measures that will strengthen its information security program.

I have enclosed a copy of the template of the notice that has been sent to the Maryland residents by U.S. mail. If you have any questions, I can be reached at (312) 915-6238 or sholler@luc.edu.

Sincerely,

Steve Holler
Associate General Counsel

Enclosures



This letter supplements the email Loyola University of Chicago (“Loyola”) sent to you on December 21, 2023, which notified you of a matter involving your personally identifiable information. It is very important that you read this letter and promptly respond, as recommended below.

On approximately November 17, 2023, Athletic Trainer Systems (“ATS”) notified Loyola and Select Physical Therapy (“SPT”) of a data security incident that had occurred. Since 2013, Loyola has retained SPT (and its predecessor, NovaCare) to provide athletic trainers to work with Loyola’s student athletes. As part of such work, SPT’s trainers log onto and enter data on an ATS software platform (the “ATS System”) to record the services provided to Loyola student athletes. Student athletes are also able to log onto the ATS System.

In its November 17, 2023 notice and in a subsequent November 30, 2023 notice, ATS reported to Loyola and SPT that weak passwords used by certain users of the ATS System “were vulnerable to brute force hack attempts” and may have been guessed by a threat actor and used to access and acquire personal information of Loyola student athletes sometime between January 2020 and January 2021. The personal information that may have been accessed may have included a Loyola student athlete’s name, date of birth, medical history, injury status, demographic information, photograph, therapy and rehabilitation referrals, COVID-19 status (including vaccinations), and Social Security number.

In December 2023, ATS provided Loyola with a list of all Loyola student athletes whose profiles appeared in the ATS System prior to January 4, 2021, which is when ATS instituted a mandatory password reset, requiring users to select a new, more complex password in order to address and correct the password vulnerability concern. You are receiving this letter because your name appeared on this list. ATS has been unable to confirm which specific student athlete profiles may have been accessed or downloaded.

To date, Loyola has no evidence that such personal information was actually used.

Although ATS has indicated that the data security incident appears to have occurred more than three years ago, if you still have an active student profile and access to the ATS System, Loyola advises you to promptly change your username and password, and any security question.

Loyola takes this incident very seriously and we are continuing to investigate this matter in order to institute additional safeguards to prevent any recurrence. Please be assured that Loyola is taking steps to increase information security awareness training as well as identifying additional technology measures that will strengthen our information security posture. Each day, Loyola monitors its systems for unlawful attacks and, on an ongoing basis, implements new technologies intended to defeat such attacks and protect the personal information of Loyola faculty, staff, and students.

In order to help protect your identity and your credit going forward, we have contracted with ConsumerInfo.com, Inc., also known as **Experian Consumer Services**, (“Experian”) to provide you with a complimentary twelve (12) month identity restoration and credit monitoring membership via Experian IdentityWorksSM. This product provides identity detection services and assistance in the resolution of identity theft.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877-890-9332**. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then, through the Identity Restoration services feature of IdentityWorksSM, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, by helping you with contacting credit grantors to dispute charges and close accounts; by assisting you in placing a freeze on your credit file with the three major credit reporting agencies; and by assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer of Experian IdentityWorksSM, including its Identity Restoration services, is available to you for

twelve (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 of Identity Restoration services are located at **www.ExperianIDWorks.com/restoration**. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary twelve (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** **_____, 2024** (Your code will not work after this date)
- **Visit** the Experian IdentityWorksSM website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code:** **INSERT CODE**

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 IdentityWorksSM online, please contact Experian's customer care team at **877-890-9332** by **_____, 2024**. Be prepared to provide **INSERT CODE** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN "IDENTITYWORKS" MEMBERSHIP

A credit card is **not** required for enrollment in Experian IdentityWorksSM.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorksSM:

- **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 ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorksSM membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

WHAT YOU CAN DO TO PROTECT YOUR INFORMATION

To further protect your information you can take steps to monitor your accounts, obtain your credit reports, or place a fraud alert or freeze on your credit account. For more information on each of these steps, please review the information below.

Monitor Your Accounts. Loyola also recommends that you remain vigilant by monitoring your financial account statements and your credit reports to reduce the chances of identity theft or fraud. You may order your free credit reports by visiting <https://www.annualcreditreport.com/index.action> or by calling 1-877-322-8228. If you notice unauthorized charges or suspect any identity theft you should report such charges or suspicions to your local police department, your state's attorney general or other state agency that assists consumers with such matters, and each credit reporting agency.

Police Report. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, you should file a police report with your local police department and obtain a copy of such report. Please note that to file a crime report or incident report with law enforcement for identity theft you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items.

Credit Freeze. You have the right to put a credit freeze (sometimes referred to as a security freeze) on your credit file, so that no new credit can be opened in your name while the freeze is in place. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax

<https://www.equifax.com/personal/credit-report-services>

1-800-685-1111

Experian

<https://www.experian.com/help/>

1-888-397-3742

TransUnion

<https://www.transunion.com/credit-help>

1-888-909-8872

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- (1) Your full name, with middle initial and any suffixes;
- (2) Your Social Security number;
- (3) Your date of birth (month, day, and year);
- (4) Your current address and your previous addresses for the past five (5) years;
- (5) Proof of your current address, such as a current utility bill or telephone bill; and
- (6) Other personal information as required by the appropriate reporting agency (consult each reporting agency's website listed above or speak with a representative of each reporting agency at their respective number listed above).

Additional Information.

You can further educate yourself regarding identity theft and the steps you can take to protect yourself by contacting your state's Attorney General, the Federal Trade Commission ("FTC"), and each of the credit reporting agencies. For example, several helpful resources provided by the FTC include the following articles: (1) What To Know About Credit Freezes and Fraud Alerts (<https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts>); (2) What to Know About Identity Theft (<https://consumer.ftc.gov/articles/what-know-about-identity-theft>); and (3) Free Credit Reports (<https://consumer.ftc.gov/articles/free-credit-reports>).

Contact information for the FTC and each of the credit reporting agencies is:

Federal Trade Commission

600 Pennsylvania Ave, NW Washington DC 20580

877-438-4338;

TTY: 1-866-653-4261

www.ftc.gov/idtheft

Equifax

1-800-525-6285

www.equifax.com

Equifax Information Services LLC

P.O. Box 105069 Atlanta, GA 30348-5069

Experian

1-888-397-3742

www.experian.com

P.O. Box 4500 Allen, TX 75013

TransUnion

1-800-680-7289

www.transunion.com

TransUnion Fraud Victim Assistance
Department

P.O. Box 2000 Chester, PA 19016

Instances of known or suspected identity theft should be reported to law enforcement, your state's Attorney General, and the FTC.

Loyola deeply regrets this situation and any inconvenience it may have created for you. If you have questions or require additional information please feel free to contact Alex Austin, athletics coordinator, at aaustin7@luc.edu or **INSERT PHONE NUMBER**.

Sincerely,
Steve Watson
Director of Athletics

* Offline members will be eligible to call Experian's customer care team for additional credit reports quarterly after enrolling in Experian IdentityWorks SM.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. ("AIG"). 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.

ADDITIONAL NOTICE TO MARYLAND RESIDENT

In addition to the notices, information, and instructions set forth in the preceding letter, you are hereby provided the following additional information pursuant to Maryland Code §14-3504(h):

- You can report any suspected identity theft to and can obtain information on how to avoid identify theft from the Federal Trade Commission (“FTC”). The FTC’s toll-free number, address, and website are listed in the attached letter.
- You can also report any suspected identity theft to and obtain information on how to avoid identify theft from the Maryland Attorney General’s Office at:

Maryland Attorney General Office

200 St. Paul Place, 25th Floor,

Baltimore, MD 21202

Phone: (410) 576-6491

idtheft@oag.state.md.us