

March 19, 2024

BY EMAIL

IDTheft@oag.state.md.us

Re: *Data Security Incident at Lawrence Technological University*

To Whom It May Concern,

I am writing to notify you regarding a data security incident. On November 17, 2023, LTU received a letter from its vendor Athletic Trainer System advising it that the vendor suffered a password reset incident around August 2020. On November 30, 2023, the vendor notified LTU regarding additional information concerning the incident, including information that the FBI had recovered some, if not all, of the bad actor's devices with student athlete information. The vendor was not able to confirm which LTU athlete profiles, if any, were actually accessed by the threat actor. On December 12, 2023, the vendor supplied LTU with a list of the LTU students whose information was contained in the affected database, which triggered LTU's own investigation regarding the incident. LTU's internal systems remained secure during the incident.

The incident involved 1499 individuals, including two (2) Maryland residents. The information involved including name, date of birth, social security number, medical information, and address.

LTU notified individuals via written letters sent on March 19, 2024. Affected individuals received complimentary credit monitoring offered through Experian for a duration of 24 months.

In response to the incident, the LTU conducted an internal investigation, engaged outside counsel, issued notifications, provided credit monitoring, and is continuing to review its processes to prevent a similar occurrence in the future. LTU's internal systems remained secure during the incident.

If there is any additional information the LTU can provide, please do not hesitate to contact me.

Very Truly Yours,

/s/ Jad Sheikali

Jad Sheikali

1 1 385 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



March 19, 2024

RE: Important Security Notification. Please read this entire letter.

Dear Sample A. Sample:

Lawrence Technological University (“LTU”) is writing to inform you regarding a data security incident. In December 2023, LTU was notified by its vendor Athletic Trainer System (“ATS”) regarding a data security incident that occurred in August 2020 where ATS received a high number of account password resets for ATS’s student athlete database. ATS was not able to confirm whether any student athlete information was accessed, and LTU’s systems were not impacted by the incident and remain secure. Out of an abundance of caution, LTU is notifying student athletes whose information was contained on the ATS database, subject to LTU’s legal notification obligations.

This letter includes instructions to enroll in complimentary credit monitoring through Experian, at no cost to you.

What Happened? In December 2023, LTU was notified by its vendor ATS regarding a data security incident that occurred in August 2020 where ATS received a high number of account password resets for ATS’s student athlete database. ATS was not able to confirm whether any student athlete information was accessed. LTU’s systems were not impacted by the incident and remain secure.

What Information Was Involved? The ATS database contained student athlete names, dates of birth, social security numbers, athletic medical information, Covid-19 status, and/or vaccination status. Based on its investigation, ATS was unable to determine whether any student athlete information was subject to unauthorized access during the incident, but LTU is taking the steps outlined in this letter out of an abundance of caution.

What Are We Doing? We take the protection of your personal information seriously. LTU systems were not impacted by this incident. We have maintained contact with our vendor ATS to determine how this issue occurred and prevent a similar reoccurrence. Following the incident, ATS performed a forced password reset on all affected accounts. We are also providing you with two years of complimentary credit monitoring through Experian, at no cost to you. The instructions to enroll in the complimentary credit monitoring are contained in this letter. At this time, LTU has no additional updates regarding this incident.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

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

Please note that Identity Restoration is available to you for 24 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 are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-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** June 30, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

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 IdentityWorks online, please contact Experian's customer care team at 833-918-8326 by June 30, 2024. Be prepared to provide engagement number B118033 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 833-918-8326 toll-free Monday through Friday 8am to 8pm Central, closed Saturday and Sunday (excluding major U.S. holidays). Be prepared to provide your engagement number B118033.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Other Steps You Can Take to Further Protect Your Information

- **Review Account Statements and Report Suspicious Activity:** Examine your account statements and credit reports for suspicious activity, and promptly notify the financial institution or company with which the account is maintained if you detect suspicious activity.

You also should promptly report any fraudulent activity or any suspected identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). For more information, visit <https://www.ftc.gov> or contact the FTC at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

- **Obtain and Monitor Credit Report:** A free copy of your credit report is available from each of the three major credit reporting agencies once every 12 months. Obtain your credit report by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>.

You can elect to purchase a copy of your credit report or receive more information by contacting one of the three national credit reporting agencies listed below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

- **North Carolina Residents.** You may obtain additional information and resources for protecting your information and identify by contacting the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000
www.ncdoj.gov

- **Consider Placing a Fraud Alert on Credit Report:** A fraud alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. The initial alert is free and will stay on your credit file for at least 90 days. Contact any of the three credit reporting agencies identified above to place a fraud alert on your credit report. For more information, visit <http://www.annualcreditreport.com> or contact the FTC or the credit reporting agencies listed above.
- **Consider Placing a Security Freeze on Credit File:** A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name and prevents potential creditors from accessing your credit report without your consent. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth,

current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze. For more information, contact the FTC and/or the credit reporting agencies listed above.