Loyola University Chicago
Information Technology Services
Granada Center • 1031 W Sheridan Rd
Chicago, Il 60660
Phone: (773) 508-4487
www.luc.edu

December 5, 2025

Dear _____

This letter is being sent to you to inform you of a data security incident that involved a small number of LOCUS accounts at Loyola University Chicago ("University"). Because your account was involved, and because of the personally identifiable information ("PII") maintained in your account, it is very important that you read this letter and promptly respond, as recommended below.

As background, the University uses a third party vendor to generate Universal IDs (UVIDs) for LOCUS account owners. A LOCUS account owner then uses their UVID to log into their LOCUS account. A flaw in the vendor's program resulted in the vendor combining data contained in an individual's UVID for a small number of LOCUS accounts. As a result, both the actual LOCUS account owner and another LOCUS user (the "Unintended User") UVIDs were allowed to access the actual LOCUS account owner's account. The total number of Unintended Users is also small and approximately equal to the number of impacted LOCUS account owners receiving this letter.

The University learned of this issue in the first half of November when an Unintended User unknowingly used a UVID with combined data to log in, and, due to the flaw, was taken to another LOCUS account owner's account. The Unintended User reported this issue to Loyola's Information Security Office (ISO). Immediately, the ISO team took investigative, containment, and remedial actions, including contacting the vendor and suspending the use of the vendor's program to generate UVIDs. In addition, and as a precaution, ITS has temporarily locked your LOCUS account to ensure your information remains secure. This is a preventative step, and we are actively working to resolve the issue as quickly as possible.

It is possible that the PII of yours listed below may have been viewed by an Unintended User, to the extent such information was present in your LOCUS account:

> **Name; phone number; bank account information; last four (4) digits of your social security number; class information and grades; financial aid, information; date of birth; and other information included in your LOCUS account.**

Your security is our top priority, and we appreciate your understanding. If you have any questions or need assistance unlocking your account, please contact Jim Pardonek, Chief Information Security Officer, Loyola University Chicago, jpardonek@luc.edu, (773) 508-6086. Thank you for your patience and trust as we continue to safeguard your information.

In order to help protect your identity and your credit going forward, Loyola has contracted with ConsumerInfo.com, Inc., also known as Experian Consumer Services ("Experian"), to provide you with a complimentary two-year 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 833-931-7577. 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, 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 reporting agencies; and 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 two years from the date of this letter. 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 two-year 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 **May 31, 2026** (Your code will not work after this date)
- Visit the Experian IdentityWorksSM website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation 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 833-931-7577 during business hours Monday through Friday by 11:59 p.m. on **May 31, 2026**. Be prepared to provide engagement number __ as proof of eligibility for the Identity Restoration services by Experian.

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

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s).

Please refer to the following resources provided by the Federal Trade Commission ("FTC"): (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). Because certain types of fraud protection may result in limitations on your ability to conduct credit transactions, it is useful to become informed about the various options available to consumers, as discussed more thoroughly in the foregoing referenced FTC resources.

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 applicable credit reporting agency. Additional information about fraud alerts and credit freezes may be obtained from the FTC and the three credit reporting agencies:

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

Loyola deeply regrets this situation and any inconvenience it may have created for you. Please feel free to contact us directly if you have questions or require additional information at datasecurity@luc.edu or contact Jim Pardonek, Chief Information Security Officer, Loyola University Chicago, jpardonek@luc.edu, (773) 508-6086.

Sincerely,

James Pardonek

Jim Pardonek, Chief Information Security Officer

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

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. 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 MASSACHUSETTS RESIDENTS

In addition to the notices, information, and instructions set forth in the preceding letter, you are hereby provided the following additional information pursuant to Massachusetts General Laws ("M.G.L.") 93H §3(b):

- Massachusetts consumers can place a security freeze on their credit report, prohibiting a credit reporting agency from releasing any information from the report without written authorization.

  Victims of identity theft must send a written request to each of the credit bureaus (Equifax, Experian, and TransUnion) by regular, certified or overnight mail and include name, address, date of birth, social security number, and credit card number and expiration date for payment, if applicable. Each credit bureau has specific requirements to place a security freeze. Review these requirements on the websites for each prior to sending your written request. (Please refer to the follow resource provided by the Federal Trade Commission: *What to Know About Credit Freezes and Fraud Alerts*, found at https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts.)

- 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. You may need such evidence to clear up any fraudulent incident.