



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Bill Garlick

Chief Information Officer

Lansing Community College | 400 North Capitol Ave., Lansing, MI 48933

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<Date>

NOTICE OF DATA BREACH

Dear <<Full Name>>:

Lansing Community College (“LCC”) is writing to inform you of an incident that may affect the privacy of some of your information. While we have no evidence of identity theft or fraud as a result of this incident, we are providing you with information about what happened, the information involved, and the steps we are taking in response. We are also including precautionary measures you can take to protect your information and details about how to obtain additional assistance, should you feel it appropriate to do so.

What Happened?

On February 18, 2025, Lansing Community College identified unauthorized access to certain systems in its network environment. After discovering the issue, LCC promptly worked with third-party specialists to secure its systems, launched an investigation and determined that an unauthorized actor had gained access through credential compromise on approximately February 12, 2025. We then further investigated the scope of the incident and the individuals whose information may have been involved. We are notifying you because information related to you was present in the impacted systems.

What Information Was Involved?

The information in the accessed system varied by individual and included personal information such as name, address, date of birth, Social Security number, driver’s license, or other information provided to or maintained by Lansing Community College. Not every affected individual had the same types of information involved. Importantly, we have no evidence at this time that any of your information was removed from our systems or misused.

What We Are Doing.

Protecting the privacy and security of personal information is a top priority for Lansing Community College. Upon learning of this incident, LCC immediately engaged independent cybersecurity experts to contain and remediate the issue, to investigate the incident in depth, and to determine exactly what information may have been impacted. Out of an abundance of caution, we have taken proactive measures to further strengthen our security protections to help ensure that incidents of this nature are less likely to occur moving forward. LCC also notified law enforcement and will notify applicable regulatory authorities where required by law. In addition to providing notice to potentially affected individuals, LCC is offering 24 months of complimentary credit monitoring and identity protection services to eligible individuals.

What You Can Do.

We encourage you to remain vigilant for signs of unauthorized activity, identity theft, and fraud. As a precaution, you may regularly review your financial account statements, credit card bills, and credit reports for any unusual or suspicious activity. You may also review the enclosed “Steps You Can Take to Help Protect Your Personal Information” for further information on other actions to safeguard your personal information. You can enroll in credit monitoring by <<Enrollment Deadline>> by taking the following steps:

- 1) Visit www.privacysolutionsid.com and click “Activate Account”;
- 2) Enter the following activation code, <<Activation Code>> and complete the enrollment form;
- 3) Complete the identity verification process;
- 4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page;
- 5) Enter your log-in credentials; and
- 6) You will be directed to your dashboard and activation is complete.

For More Information.

We understand that you may have questions not addressed in this letter. If you have additional questions or need further information, please call our dedicated assistance line at 866-659-7088 (toll-free), Monday through Friday, 9:00 A.M. – 9:00 P.M. Eastern Time. You may also write to Lansing Community College at 411 N. Grand Avenue, Attn: Risk Management, JR Beauboeuf, Lansing, MI 48933. Our representatives are available to assist you and provide additional information.

Sincerely,

Lansing Community College



William Garlick
Chief Information Officer

Enclosure: “Steps You Can Take to Help Protect Your Personal Information”

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Credit Monitoring Services. If you need assistance with the enrollment process or have questions regarding credit monitoring, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET. The following product features are included in the credit monitoring:

- **1-Bureau Credit Monitoring with Alerts:** Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.
- **Dark Web Monitoring (Basic):** Monitors one email address, phone, name, DOB, and SSN on the dark web. Includes retrospective report as well as ongoing monitoring.
- **Credit Protection:** 3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).
- **Change of Address Monitoring:** Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.
- **Identity Restoration & Lost Wallet Assistance:** Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Monitor Your Accounts and Credit Reports. Under U.S. law, you are entitled to receive free weekly online credit reports from each of the three major credit reporting bureaus (Equifax, Experian, and TransUnion). To request your free credit reports call 1-877-322-8228 or visit www.annualcreditreport.com. We encourage you to use this resource and remain vigilant by monitoring your account statements and credit reports for any unexpected activity. You have the right to place an initial or extended "fraud alert" on your credit file at no cost. An initial fraud alert lasts one year and will prompt creditors to take steps to verify your identity before extending credit. If you are the victim of identity theft, you are entitled to an extended fraud alert, which stays on your credit file for seven years. To place a fraud alert, contact any one of the three major credit bureaus using the contact information below. (The bureau you contact will notify the other two.) As an alternative to a fraud alert, you also have the right to place a security freeze (also known as a credit freeze) on your credit report to restrict access to your credit file. A security freeze is free of charge and prevents new credit from being opened in your name without your approval. Please be aware that a freeze may delay or prevent approval of any new credit or loans until you lift the freeze. To request a security freeze, you may need to provide some or all of the following information (which may vary if you request online, by phone, or by mail):

- Full name (including any suffixes such as Jr., Sr., II, III, etc.)
- Social Security number
- Date of birth
- Addresses for the past 2-5 years, and roof of current address (such as a recent utility bill or telephone bill)
- A photocopy of a government-issued ID card (such as a driver's license or state ID)
- If you are an identity theft victim, a copy of a police report, investigative report, or complaint that you filed with a law enforcement agency about identity theft

If you wish to place a fraud alert or to obtain credit freeze, you can contact the three major credit bureaus using the information below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/credit-freeze	www.experian.com/freeze	https://www.transunion.com/credit-freeze
1-888-378-4329	1-888-397-3742	1-800-916-8800
Equifax Information Services P.O. Box 105788 Atlanta, GA 30348-5788	Experian P.O. Box 9554 Allen, TX 75013	TransUnion P.O. Box 160 Woodlyn, PA 19094

Additional Resources: The Federal Trade Commission (FTC) may be reached at 1-877-ID-THEFT (1-877-438-4338), and additional information is available at www.identitytheft.gov or by writing to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint using the above contact information. Consumers have the right to file a police report or their state Attorney General if they experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. This notice has not been delayed by law enforcement.

State-Specific Information:

- For District of Columbia residents: You may contact the District of Columbia Office of the Attorney General at 400 6th Street, NW, Washington, D.C. 20001, 202-727-3400, or oag.dc.gov for information on steps to take to protect yourself from identity theft.
- For Maryland residents: You may contact the Maryland Office of the Attorney General at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023 (toll-free) or 1-410-528-8662, or via the website www.marylandattorneygeneral.gov for guidance on identity theft protection.
- For New Mexico residents: You have rights under the Fair Credit Reporting Act (FCRA), including the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to request your credit score, and the right to dispute incomplete or inaccurate information. Under the FCRA, consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to third parties; and you may limit “prescreened” offers based on your credit information. If you are an identity theft victim or active duty military, you have specific additional rights under the FCRA. We encourage you to review your rights by visiting <https://www.consumerfinance.gov/learnmore/> or writing to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.
- For New York residents: You may contact the New York State Office of the Attorney General at The Capitol, Albany, NY 12224-0341, 1-800-771-7755, or ag.ny.gov for information on security breach response and identity theft prevention.
- For North Carolina residents: You may contact the North Carolina Attorney General’s Office at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 (toll-free in North Carolina) or 1-919-716-6000, or www.ncdoj.gov to obtain information about preventing identity theft.
- For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General at 150 South Main Street, Providence, RI 02903, 1-401-274-4400, or www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. Additionally, approximately 30 Rhode Island residents were affected by this incident.