

Notice of Data Breach

October 07, 2025: Lincoln University takes the privacy and security of our community's personal information seriously. We are notifying you of a data security incident that may have involved personal information of certain Lincoln University current and former employees, students, and applicants. We were unable to locate all the addresses of the individuals whose information was involved. As a result, we are issuing this public notice to inform all potentially involved individuals of the incident. This notice explains the incident, our response, and steps you can take to help protect your personal information.

What Happened: On October 9, 2024, we became aware of a disruption to our computer network. We took immediate action to secure our systems. We partnered with cyber incident response professionals to investigate the nature and scope of the incident. As part of the investigation, we learned that certain data was likely taken from our network by an unauthorized actor. After a comprehensive review, on May 2, 2025, we learned that certain files within that data set contained personal information. We then engaged in a process to identify last known contact information for individuals which was completed on September 22, 2025.

What Information Was Involved: The information that was involved varies by individual, but may have included individuals' first and last name, in combination with one or more of the following data element(s): Social Security number, driver's license or state identification card number, passport number, individual taxpayer identification number, date of birth, and/or student identification number.

What We Are Doing: Upon learning of the incident, we took immediate steps to address it, including securing our systems. We partnered with cyber incident response professionals and notified federal law enforcement. We are reviewing our existing security policies and protections already in place on our network and adopting additional security to safeguard against evolving threats moving forward.

If you believe your information may have been affected by this incident and have not received a notification letter from us, please do not hesitate to contact our dedicated assistance line through HaystackID at 888-844-1265 (toll free) between the hours of 8:00 a.m. and 11:00 p.m. EST. In addition, as an added protection, we are offering complimentary credit monitoring and identity protection services through HaystackID to individuals whose Social Security numbers were involved. To confirm eligibility and enroll, please contact the dedicated assistance line..

What You Can Do: As a general matter, it is important to be vigilant against incidents of identity theft and fraud, from any source, by periodically reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, promptly contact the financial institution or service provider. You may also file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the below "*Steps You Can Take to Help Protect Your Information*" for additional resources you may take advantage of to protect against fraud and identity theft, should you find it appropriate to do so.

For More Information: Should you have any questions or concerns, please contact our dedicated assistance line with HaystackID at 888-844-1265 (toll free), during the hours of 8:00 am to 11:00 pm Eastern time, Monday through Friday and 9:00 am to 6:00 pm Saturday (excluding U.S. national holidays). Please know that the security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

Lincoln University

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts and Credit Reports:

It is good practice to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors.

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alert Services:

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Credit Freeze Instructions:

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1- 800-916-8800 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-378-4329 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
--	---	--

Additional Information:

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For D.C. Residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>.

For Maryland Residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For New Mexico Residents, you have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

For New York Residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina Residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is one (1) Rhode Island resident whose data was involved in this incident.