





March 24, 2025

Subject: Notice of Data << Variable Text 1>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a recent data security incident that may have involved your information. Lee University takes the privacy and security of all information in our possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your information.

What Happened. In March 2024, we experienced a security incident that impacted our local systems through a third-party software vulnerability. After detecting the third-party vulnerability and containing the incident, we launched an investigation with the support of industry-leading cybersecurity experts to learn more about the scope of the potentially affected data on those systems. Our investigation revealed that some university data may have been downloaded from our systems. We then launched a comprehensive review of all potentially affected data to try to identify individuals whose information was involved and gather contact information needed to provide notice. These efforts concluded in March 2025. After we learned that some of your information was potentially involved, we arranged to provide you this notice.

What Information Was Involved. The potentially involved information varies by individual. Based on the investigation, we understand that the information may have included your << Variable Text 2>>.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. As part of our ongoing commitment to information security, we are reviewing existing policies and procedures and implementing enhanced security measures to reduce the likelihood of a similar incident occurring in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information.

In addition, we are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. You can follow the recommendations on the following page to help protect your information. We also encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-877-719-6522, visiting https://app.idx.us/account-creation/protect or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is June 24, 2025.

As a precautionary measure, the Lee University recommends that you remain vigilant by reviewing your account statements and credit reports closely. Consider changing passwords for your accounts. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-877-719-6522, Monday through Friday from 9 am - 9 pm Eastern Time. Representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

We understand and regret the concern and inconvenience of this situation. Please be assured that we are taking this incident seriously. The privacy and protection of information we store is a top priority of ours.

Sincerely,

Lee University

1120 N Ocoee Street Cleveland, TN 37311

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Internal Revenue Service Identity Protection PIN (IP PIN): You may obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service – a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Information about the IP PIN program can be found here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com TransUnion
P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

Security Freeze: You have the right to put a security freeze on your credit file at no cost. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order 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. For TransUnion: www.transunion.com/credit-freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov 877-438-4338 Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/
Pages/CPD
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumerprotection
877-877-9392

California Attorney General

1300 I Street Sacramento, CA 95814 www.oag.ca.gov/privacy 800-952-5225

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

Kentucky Attorney General

700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601 www.ag.ky.gov 502-696-5300

New York Attorney General

The Capitol Albany, NY 12224 800-771-7755 ag.ny.gov

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

NC Attorney General

9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov/protectingconsumers/ 877-566-7226

Rhode Island Attorney General

150 South Main Street Providence, RI 02903 www.riag.ri.gov 401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW Washington, DC 20001 oag.dc.gov/consumer-protection 202-442-9828

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.