CONSTANGY BROOKS, SMITH & PROPHETE LLP

Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

March 25, 2025

VIA EMAIL: DOJ-CPB@doj.nh.gov
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notification of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP represents Lee University in connection with a data security incident described in greater detail below. Lee University is a private Christian university located in Cleveland, Tennessee. Lee University takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification statute, N.H. Rev. Stat. §§ 359-C:19 to C:21.

1. **Nature of the Security Incident**

On March 19, 2025, Lee University learned that some personal information relating to its students, donors, and current or former employees was contained within a data set which was subject to a data security incident. Lee University discovered a cybersecurity incident on March 22, 2024, and immediately began an investigation of the matter with the assistance of engaged independent cybersecurity experts. The investigation determined that files containing personal information may have been accessed or acquired without authorization. Lee University then undertook an investigation to understand whether data was potentially involved and, if so, what that data was so that notification could be provided. The comprehensive review and processes needed to identify contact information for potentially affected concluded on March 19, 2025. As a result of that investigation, Lee University learned that some personal information of individuals was contained within the involved data.

2. **Number of Affected New Hampshire Residents & Information Involved**

The investigation of the incident revealed that it may have involved personal information for approximately 139 New Hampshire residents. The information involved in the incident may differ depending on the individual but may include the following for affected New Hampshire residents:

.

3. **Notification to Affected Individuals**

On March 24, 2025, notification letters were sent to affected New Hampshire residents by USPS First Class Mail.

The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers of complimentary identity protection services to each New Hampshire resident whose Social Security number was affected by this event, including credit monitoring, dark web monitoring, $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed.

4. **Measures Taken to Address the Incident**

Upon discovering this incident, in addition to taking the steps described above, Lee University took steps to secure its systems and launched an investigation to learn more about what happened and what information could have been affected. Lee University also took immediate steps to evaluate and improve the security of its systems and will continue to evaluate additional protections that can be put into place to supplement its existing security policies and procedures. In addition, Lee University took measures to provide preliminary notice via email to potentially affected individuals before completion of its data review, beginning in November 2024. Additional preliminary notice was published on the Lee University website.

Lee University has established a toll-free call center through IDX to answer questions about the incident and address related concerns. Finally, Lee University notified the potentially affected individuals and provided them with steps they can take to protect their personal information and reported the incident to nationwide consumer reporting agencies (i.e., Equifax, Experian, and Transunion).

5. **Contact Information**

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at .

Sincerely,

Aubrey Weaver
Partner, Cybersecurity & Data Privacy Team

AW:MFF

Encl.: Sample Notification Letter

Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

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: 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 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 .

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/consumer-protection
877-877-9392

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

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

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

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

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

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

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

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

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.

Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

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.

What You Can Do. You can follow the recommendations on the following page to help protect your information.

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	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-833-799-5355
www.equifax.com	www.experian.com	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	**Maryland Attorney General**	**Oregon Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	1162 Court St., NE
Washington, DC 20580	Baltimore, MD 21202	Salem, OR 97301
consumer.ftc.gov	www.marylandattorneygeneral.gov/Pages/CPD	www.doj.state.or.us/consumer-protection
877-438-4338	888-743-0023	877-877-9392

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

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

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

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

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

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

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

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

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.