THE UNIVERSITY OF ALABAMA® | *Office of* Information Technology

September 21, 2021

Attorney General John M. Formella
DOJ-CPB@doj.nh.gov
NH Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Attorney General John M. Formella,

I am writing to notify your office of a security incident involving one (1) New Hampshire resident. The University of Alabama ("UA") has learned of a security incident involving a laptop belonging to one of our employees which may have resulted in unauthorized access to a document that contained personally identifiable information ("PII"). We anticipate sending a notice to affected individuals on September 24, 2021. A copy of that letter is attached.

On August 26, 2021, a personal laptop belonging to a UA employee was stolen. The UA employee's email account was synced to the laptop. UA officials immediately conducted a scan of the employee's email account to determine if sensitive or confidential information was contained in the email account. UA discovered the employee's email account contained a single document that included PII for approximately 185 employees and 112 dependents of employees. Specifically, this document included data for employees eligible for COBRA health insurance: name, address, phone number, social security number, date of birth, gender, and other less sensitive benefits, benefit eligibility and employment-related information such as participant ID numbers, member numbers, hire and separation dates, qualifying event description, benefit type, coverage dates, and similar data. No credit card or banking information was included on this document. The laptop was protected by a password; however, because the laptop was personal equipment and not University-owned and supported equipment, UA cannot guarantee that the laptop was encrypted and that the information was inaccessible. While we have no indication that the information was accessed, viewed, or used in any way, the opportunity for it to be seen existed.

Please know that the University of Alabama takes this incident seriously, and we are committed to doing all we can to keep this from happening again. The University constantly reviews and updates the comprehensive plan we have in place to secure sensitive information, and we are committed to continuing to do so, including reminding employees of preventive measures they can take to reduce the risk of this type of incident.

Please do not hesitate to call or email me if you have any questions.

Taylor B. Anderson
Deputy Chief Information Security Officer
The University of Alabama
205-348-6946 | tbanderson@ua.edu

The University of Alabama

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

THE UNIVERSITY OF ALABAMA®

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

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

September 24, 2021

Notice of Data Breach

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

We are contacting you because of a security incident that occurred on August 26, 2021, which may have resulted in unauthorized access to a document that contained personally identifiable information about you. We want to let you know what happened, what information was potentially accessed, what we are doing to minimize the potential for access, and provide you with additional steps you can take in response.

WHAT HAPPENED?
On August 26, 2021, a personal laptop belonging to a UA employee was stolen. The UA employee's email account was synced to the laptop. UA officials immediately conducted a scan of the employee's email account, which included tens of thousands of emails, to determine if sensitive or confidential information was contained anywhere in the email account. UA discovered the employee's email account included an email with an attachment containing one single document that included personally identifiable information for approximately 185 employees and 112 dependents of employees.

The laptop was protected by a password; however, because the laptop was personal equipment and not University-owned and supported, UA cannot guarantee that the laptop was encrypted. While we have no indication that the information was viewed or used in any way, the opportunity for it to possibly be seen existed, so we wanted to let you know. We also want to make sure you are aware of proactive measures you can take to protect yourself from any possible misuse of your sensitive information.

WHAT INFORMATION WAS INVOLVED?
Specifically, the document identified as containing personally identifiable information included data for employees and their dependents eligible for COBRA insurance. This document included your name, address, phone number, social security number, date of birth, gender, and other less sensitive benefits, benefit eligibility and employment-related information such as participant ID numbers, member numbers, hire and separation dates, qualifying event description, benefit type, coverage dates, and similar data. No credit card or banking information was included on this document.

WHAT YOU CAN DO.
The University is offering you two years of free credit monitoring and identity theft detection services. These services are available at no charge to you. More information about these services, including how to enroll in these services, is included on the enclosure to this letter.

We do not have any evidence that your information was accessed or used. However, and even if you choose not to take advantage of this free membership, we have included in the enclosure other additional credit safety tips you may wish to use at any time to help protect yourself from any possible misuse of your information.

WHAT WE ARE DOING.
First, we apologize for any inconvenience or concern this incident may cause you. We are bringing this to your attention so that you can be alert to signs of any possible misuse of your information.

Please know that I and the entire UA administration take this incident seriously, and we are committed to doing all we can to keep this from happening again. In this instance, the laptop was password protected, and it has been set to remotely erase all information if and when it is connected to the internet again. The University constantly reviews and updates the comprehensive plan we have in place to secure sensitive information, and we are committed to continuing to do so, including reminding employees to not store sensitive information on personal computers or on unencrypted mobile devices.

FOR MORE INFORMATION
You will find detailed instructions for enrollment in the credit monitoring and identity theft detection services mentioned on the enclosed Recommended Steps document. Please do not discard this letter, as you will need to reference the enrollment code at the top of this letter should you decide to call or enroll.

Please call 1-800-939-4170 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have. Agents are available Monday through Friday, 8 am to 8 pm Central Time.

Sincerely,
Nancy Whittaker

Associate Vice President for Human Resources

CREDIT MONITORING SERVICES PROVIDED:

- **Single Bureau Credit Monitoring** - Monitoring of credit bureau for changes to the individual's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers and other activities that affect the individual's credit record.

- **Cyberscan** - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

- **Identity Theft Insurance** - Identity theft insurance will reimburse individuals for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

- **Fully-Managed Identity Recovery** – IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned ID Care Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

  To activate your credit monitoring and identity theft detection, please follow the steps below.
  - Visit the IDX website to enroll: https://app.idx.us/account-creation/protect.
  - Provide your unique activation code <<XXXXXXXX>>.
  - Ensure that you enroll by December 24, 2021. Your unique activation code will not work after this date.

Additional Credit Safety Tips

We encourage all individuals to always actively monitor their credit for the possibility of fraud and identity theft by reviewing credit reports, and credit card, bank and other financial statements for unauthorized activity.

- **Fraud Alert:** Place a fraud alert on your account with the three credit bureaus listed below. This free service will automatically notify you before new accounts can be opened in your name, or before creditors can make changes to your existing accounts. You can activate fraud alerts by contacting any of the three nationwide credit bureaus listed below. The fraud alert will automatically be sent to the other two credit bureaus.
  - Transunion: PO Box 2000, Chester, PA 19016; 1-800-680-7289; www.transunion.com
  - Equifax: PO Box 105069, Atlanta, GA, 30348-5069; 1-800-525-6285; www.equifax.com
  - Experian: PO Box 2002, Allen, TX 75013; 1-888-397-3742; www.experian.com

- **Credit Freezes**: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:
  - Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html
  - TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com/credit-freeze
  - Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com/personal/credit-report-services/

  To request a security freeze, you will need to provide the following information:
  - Full name

- Social Security number
- Date of birth
- If you have moved in the past five years, provide the addresses where you have lived over the prior five years
- Proof of current address, such as a utility bill
- A photocopy of a government issued ID
- If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

- It is always advisable to be vigilant for incidents of fraud or identity theft by regularly reviewing all your account statements and monitoring free credit reports for unusual or unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three credit reporting companies above. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

- Contact law enforcement immediately - if you believe that your personal information has been fraudulently used.

- If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. Contact information for the Federal Trade Commission is as follows:
  - Federal Trade Commission, Consumer Response Centre, 600 Pennsylvania Avenue NW, Washington, DC 20580
  - FTC Identify Theft Hotline: 1-877-IDTHEFT (438-4338)
  - FTC Identify Theft Website: http://www.ftc.gov/idtheft

- The Social Security Administration also maintains a fraud hotline at 1-800-269-0271.

- **You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

  - **California Residents:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

  - **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

  - **Maryland Residents:** Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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

  - **North Carolina Residents:** Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

  - **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

  - **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

  - **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.