MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

James Monagle
Office: (267) 930-1529
Fax: (267) 930-4771
Email: jmonagle@mullen.law

178 East Hanover Ave, #103-373
Cedar Knolls, NJ 07927-2013

December 15, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Sir or Madam:

We represent Claremont Lincoln University ("CLU") located at 150 W 1st Street, Claremont, CA 91711, and are writing to notify your Office of an incident that may affect the security of some personal information relating to two (2) New Hampshire residents. By providing this notice, CLU does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 29, 2020, CLU became aware of unusual activity relating to an employee email account. CLU immediately commenced an investigation with the assistance of third-party computer specialists. On July 28, 2020, the investigation determined that certain CLU email accounts were accessed without authorization at varying times from June 1, 2020 to July 2, 2020. CLU promptly began a thorough review of the contents of the accounts to determine whether sensitive information was present at the time of the incident. On September 25, 2020, CLU determined that personal information as defined N.H. Rev. Stat. 359-C:19 was present in the affected email accounts at the time of the incident, which included name and Social Security number. To date, the investigation has found no evidence of actual or attempted misuse of personal information as a result of this incident.

Notice to New Hampshire Residents

On December 15, 2020, CLU provided written notice of this incident to affected individuals, which include two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of this incident, CLU promptly changed the email account credentials and investigated to confirm the security of its email network. After the investigation had determined that email accounts were potentially accessible, CLU moved quickly to review the accounts for sensitive information. The preliminary review confirmed the accounts contained some sensitive information, but they did not contain address information for many of individuals associated with this information. As such, CLU is reviewing its internal records and working with a third party to identify address information for purposes of providing notification of this incident. Upon the completion of this review, CLU will provide notice to potentially affected individuals.

As part of its ongoing commitment to data security, CLU is also taking steps to enhance its data security; these include reviewing existing policies and procedures, conducting additional employee training, and implementing additional security measures.

Should you have any questions regarding this preliminary notification, please contact us at (267) 930-1529.

Very truly yours,

James Monagle of
MULLEN COUGHLIN LLC

JZM/jc1

Exhibit A

CLAREMONT LINCOLN UNIVERSITY
Socially Conscious Education®

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

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>>

December 15, 2020

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

What Happened

Claremont Lincoln University ("CLU") writes to notify you of a recent incident that may affect the security of some of your personal information. While there is currently no evidence that your information has been misused as a result of this incident, we are providing you with information on the event, measures we have taken, and what you may do to better protect your personal information should you feel it appropriate to do so.

What Happened? On June 29, 2020, CLU became aware of unusual activity relating to an employee email account. CLU immediately commenced an investigation with the assistance of third-party computer specialists. On July 28, 2020, the investigation determined that certain CLU email accounts were accessed without authorization at varying times from June 1, 2020 to July 2, 2020. CLU promptly began a thorough review of the contents of the accounts to determine whether sensitive information was present at the time of the incident. On September 25, 2020, we determined that some of your information was present in at least one of the involved email accounts. To date, CLU is unaware of any actual or attempted misuse of your information as a result of this incident.

What Information Was Involved? CLU 's investigation confirmed the information present within the impacted accounts at the time of the incident includes your name and <<POTENTIAL DATA ELEMENTS>>. Please note that while our investigation did not reveal evidence that your information was actually viewed by the unauthorized actor, we are providing you this notice to ensure you are aware of this incident.

What We Are Doing. Information, privacy, and security are among our highest priorities. CLU has strict security measures in place to protect information in our care. Upon learning of this incident, we promptly changed the email account credentials and investigated to confirm the security of our email network. We are also taking steps to enhance our data security; these include reviewing existing policies and procedures, conducting additional employee training, and implementing additional security measures.

Although we are unaware of any actual or attempted misuse of your information as a result of this incident, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Instructions on how to enroll can be found within the enclosed "Steps You Can Take to Protect Personal Information." Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity for the next twelve (12) to twenty-four (24) months. You may review the information contained in the enclosed "Steps You Can Take to Protect Personal Information." You may also enroll to receive the identity and credit monitoring services we are making available to you as we are unable to enroll in these services on your behalf.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, we established a dedicated assistance line at 1-800-939-4170 which can be reached Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. You may also contact CLU by mail at 150 W 1st Street, Claremont, California 91711.

Sincerely,

Anthony F. Digiovanni
President
Claremont Lincoln University

Steps You Can Take to Protect Your Personal Information

Enroll in Credit Monitoring

Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is March 15, 2021.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Chester, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	**www.transunion.com/credit-freeze**	**www.equifax.com/personal/credit-report-services**

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, 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, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as 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 ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For 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, and https://ag.ny.gov/.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, and www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<XX>> Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, 1-202-442-9828, and https://oag.dc.gov