MULLEN COUGHLIN LLC

James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

December 20, 2016

**VIA U.S. MAIL**
Office of the Attorney General
Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319



Re: **Notice of Data Security Incident**

Dear Sir/Madam:

We represent Luther College, 700 College Drive, Decorah, Iowa 52101, and are writing to notify you of a data security incident that may affect the security of personal information of one thousand fifty-three (1,053) Iowa residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Luther College does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

**Nature of the Data Security Event**

On October 12, 2016, Luther College discovered that it had become the target of a phishing email campaign and that a few Luther College employees had clicked on the phishing emails and entered their credentials. Luther College immediately took steps to secure these employees' computers and email accounts and launched an in-depth investigation to determine whether any sensitive information was accessed or acquired. On November 1, 2016, Luther College determined, with the help of outside computer forensic investigators, that an unknown individual or individuals had gained access to the workstation computer files and email accounts of the Luther College employees. Upon learning of this incident, Luther College immediately launched an investigation to determine what information, if any, was subject to unauthorized access or acquisition. This has involved a time consuming, manual review process.

Luther College takes the security of information in its care very seriously. While there is no evidence that the individual(s) accessed or acquired personal information from the employees'

computer applications or email accounts, access to the information contained therein could not be ruled out. These computer applications and email accounts may have contained the name, date of birth, address, Social Security Number, and financial account information, of the affected Iowa residents.

**Notice to Iowa Residents**

On or about December 19, 2016, written notice will be provided to the one thousand fifty-three (1,053) residents whose information was accessible to the intruder, in substantially the same form as the letter attached hereto as ***Exhibit A***.

**Other Steps Taken and To Be Taken**

In addition to providing written notice of this incident to all affected individuals as described above, Luther College is offering all affected individuals access to 12 months of complimentary credit monitoring and identity restoration services with AllClear ID, and is providing these individuals with helpful information on how to protect against identity theft and fraud. Luther College is also providing written notice of this incident to other state regulators and consumer reporting agencies, where required. To prevent another incident of this kind from happening, Luther College has hired an outside computer forensic investigator to confirm the security of its systems and to make recommendations for improving Luther College's overall security posture.

**Contact Information**

Should you have any questions regarding this notification or other aspects of this data security incident, please contact us at (267) 930-4798.

Very truly yours,

James E. Prendergast of
MULLEN COUGHLIN LLC

# EXHIBIT “A”

LUTHER COLLEGE

Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001
ACD1234

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

December 19, 2016

**Re: Notice of Data Breach**

Dear John Sample:

On behalf of Luther College, I am writing to inform you of a recent incident that may affect the security of your personal information. While we are unaware of any actual or attempted misuse of your personal information, we are providing you with information about the incident, steps we are taking in response, and steps you can take to protect against fraud should you feel it is appropriate.

***What Happened?*** On October 12, 2016, we discovered that Luther College had become the target of a phishing email campaign and that a few Luther College employees had clicked on the phishing emails and entered their credentials. We immediately took steps to secure these employees' computers and email accounts and launched an in-depth investigation to determine whether any sensitive information was accessed or acquired. On November 1, 2016, we determined, with the help of outside computer forensic investigators, that an unknown individual or individuals had gained access to the workstation computer files and email accounts of Luther College employees. These workstation computer files and email accounts contained, among other things, personally identifiable information of certain individuals related to Luther College. While we have no evidence that anyone accessed or acquired personally identifiable information, access to the information on the workstation computer or email accounts cannot be ruled out.

***What Information Was Involved?*** While we have no evidence that the unauthorized individual or individuals actually accessed or acquired your information, we have confirmed that your name and Bank Account Number, Bank Name were accessible to the intruder.

***What We Are Doing.*** We take the security of information in our care very seriously. We have been working diligently since November 1 to determine what information was contained in the email accounts and computer files subject to the unauthorized access. In addition to launching an investigation into this incident, we have hired an outside computer forensic investigator to supplement our internal investigation, and to confirm the security of our computer systems. This has involved a time consuming, manual review process. Now that the review is complete, we are providing notice of this incident to all potentially impacted individuals.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-220-9438 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-220-9438 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

We are also providing required notice of this incident to appropriate state regulators and consumer reporting agencies.

***What You Can Do.*** Please review the enclosed Privacy Safeguards Information for additional information on how to better protect against identity theft and fraud. You may also enroll in the complimentary credit monitoring and identity restoration services.

***For More Information***. We are very sorry for any inconvenience or concern this incident causes you. The security of your information is a priority for us. Should you have any questions about the content of this letter or ways you can better protect yourself from the possibility of identity theft, we encourage you to call the dedicated assistance line, staffed by professionals who are experienced in working through situations like this, at 1-855-220-9438 between 8:00 a.m. and 8:00 p.m. CST, Monday through Saturday, excluding major holidays.

Sincerely,

Eric Runestad
Vice President for Finance and Administration
Luther College

## PRIVACY SAFEGUARDS INFORMATION

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-220-9438 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-220-9438 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. 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.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

| Equifax | Experian | TransUnion |
|---|---|---|
| P.O. Box 105069 | P.O. Box 2002 | P.O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19022-2000 |
| 800-525-6285 | 888-397-3742 | 800-680-7289 |
| www.equifax.com | www.experian.com | www.transunion.com |

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

| Equifax Security Freeze | Experian Security Freeze | TransUnion |
|---|---|---|
| P.O. Box 105788 | P.O. Box 9554 | P. O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19022-2000 |
| 800-685-1111 | 888-397-3742 | 888-909-8872 |
| (NY residents please call 1-800-349-9960) | www.experian.com/freeze/center.html | www.transunion.com/securityfreeze |
| www.freeze.equifax.com | | |

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting 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. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 1 Rhode Island resident may be impacted by this incident. Customers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, customers will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed as a result of a law enforcement investigation.

# AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

**Services Provided**
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

**Coverage Period**
Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

**Eligibility Requirements**
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

**How to File a Claim**
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

**Coverage under AllClear Identity Repair Does Not Apply to the Following:**
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

**Other Exclusions:**

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

**Opt-out Policy**
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

| E-mail | Mail | Phone |
|---|---|---|
| support@allclearid.com | AllClear ID, Inc.<br>823 Congress Avenue Suite 300<br>Austin, Texas 78701 | 1.855.434.8077 |

MULLEN
COUGHLIN

1275 Drummers Lane, Suite 302
Wayne, PA 19087

PHILADELPHIA PA 191
28 DEC 2016 PM 2 L

Office of the Attorney General
Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319

50319-010999