

STATE OF NH  
DEPT OF JUSTI  
2018 JUN 29 AM 10:40



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

James E. Prendergast  
Office: 267-930-4798  
Fax: 267-930-4771  
Email: [jprendergast@mullen.law](mailto:jprendergast@mullen.law)

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

June 22, 2018

**VIA U.S. MAIL**

Attorney General Gordon J. MacDonald  
Office of the New Hampshire Attorney General  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Security Incident**

Dear Attorney General Gordon J. MacDonald:

We represent Tuskegee University ("Tuskegee") located at 1200 W Montgomery Road, Tuskegee, AL and are writing to notify your office of an incident that may affect the security of some personal information relating to New Hampshire residents. By providing this notice, Tuskegee 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 or about March 12, 2018, Tuskegee became aware of suspicious activity regarding faculty and staff email accounts. Tuskegee immediately launched an investigation to confirm the security of their network and to determine the nature and scope of this event. With the assistance of third-party forensic investigators, Tuskegee learned they were the victim of an email phishing attack which resulted in unauthorized access to certain faculty and staff email accounts. The investigation determined that 48 Tuskegee faculty and staff email accounts had unauthorized access between September 24, 2017 and March 22, 2018.

It was recently determined that the information that could have been subject to unauthorized access includes name, address and Social Security number .

### **Notice to New Hampshire Residents**

On or about June 21, 2018, Tuskegee began providing written notice of this incident to all affected individuals, which includes 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 discovering the event, Tuskegee moved quickly to investigate and respond to the incident, assess the security of Tuskegee systems, and notify potentially affected individuals. Tuskegee is also working to implement additional safeguards and training to its employees.

Tuskegee is providing access to credit monitoring services for one (1) year, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Tuskegee is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Tuskegee is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

### **Contact Information**

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

Very truly yours,



James E. Prendergast of  
MULLEN COUGHLIN LLC

JEP/alc  
Enclosure

# EXHIBIT A



TUSKEGEE UNIVERSITY

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<ZipCode>>

## Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

Tuskegee University ("Tuskegee") is writing to notify you of an incident that may affect the security of your personal information. We are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect identify theft and fraud.

**What Happened?** On March 12, 2018, Tuskegee became aware of suspicious activity regarding faculty and staff email accounts. We immediately began an investigation to confirm the security of our network and to determine the nature and scope of this event. With the assistance of third-party forensic investigators, we learned Tuskegee was the victim of an email phishing attack which resulted in unauthorized access to certain faculty and staff email accounts between September 24, 2017 and March 22, 2018. Based upon available forensic evidence, it appears an email containing your personal information was subject to unauthorized access. To date, we have no evidence of actual or attempted misuse of information. We are notifying you in abundance of caution since this information was present in the impacted email accounts.

**What Information Was Involved?** Our investigation determined the following types of your personal information were stored within an impacted email account and may have been subject to unauthorized access: <<ClientDef1(name and [data elements].)>>

**What We Are Doing.** Tuskegee takes your privacy and security of personal information seriously. We are continuously taking steps to enhance data security protections to protect information with our care. As part of our incident response, we changed the log-in credentials for those email accounts impacted by this incident to prevent further unauthorized access. Since then, we have continued ongoing efforts to enhance security controls and to implement additional controls, including use of multi-factor authentications to help protect employee email accounts from unauthorized access.

As an added precaution, we are offering you access to 12 months of free credit/identity monitoring and identity restoration services through Experian. We encourage you to take advantage of these identity protection services.

**What You Can Do.** You can review the attached *Steps You Can Take to Protect Against Identity Theft and Fraud*. You can also enroll to receive the free services being offered to you.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. We have established a confidential, toll-free hotline to assist you with questions regarding this incident, the free services we are making available, and steps you can take to protect yourself against identity theft and fraud. The hotline is available Monday through Friday, 8:00 a.m. to 5:00 p.m., CT, at 1-866-323-7897.

We sincerely regret the inconvenience this incident causes for you. Tuskegee remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

A handwritten signature in black ink, appearing to read "James Cooper". The signature is stylized and cursive.

James Cooper  
Interim Chief Information Officer  
Tuskegee University

Enclosure

## Steps You Can Take to Protect Against Identity Theft and Fraud

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

### Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **October 1, 2018** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the Activation Code: <<Member ID>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **DB07121** as proof of eligibility for the identity restoration services by Experian.

### ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.**

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

**Credit Reports.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free 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](http://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.

**Fraud Alerts.** 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  
P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285  
www.equifax.com

Experian  
P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
www.experian.com

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
www.transunion.com

**Security Freeze.** 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. Fees vary based on where you live, but commonly range from \$3 to \$15. 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. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
www.freeze.equifax.com

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
www.experian.com/freeze/

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
freeze.transunion.com

**Additional Information.** You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud 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](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. This notice has not been delayed as the result of a law enforcement investigation. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023. Employee Benefits is located at 1350 Deming Way, Suite 300, Middleton, Wisconsin 53562; and [www.oag.state.md.us](http://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](http://www.ncdoj.gov). **For Rhode Island Residents:** The Rhode Island Attorney General may be contacted at: Rhode Island Attorney General's Office, 150 South Main St., Providence, RI 02903. <http://www.riag.ri.gov>. Approximately 3 Rhode Island residents may have been affected by this incident. **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 violator. 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](http://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. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.