



MULLEN
COUGHLIN^{LLC}

STATE OF NH
DEPT OF JUSTICE

2017 JAN 17 AM 11: 54

Claudia D. McCarron
Office: 267-930-4787
Fax: 267-930-4771
Email: cmccarron@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

January 10, 2017

VIA U.S. MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Mr. Foster:

Our office represents Haverford College ("Haverford"), 370 Lancaster Avenue, Haverford, PA 19041. We are writing to provide you with notice of an event that may impact the security of personal information relating to one (1) New Hampshire resident. By providing this notice, Haverford College does not waive any rights or defenses regarding the applicability of New Hampshire law, applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Background

On August 2, 2016, Haverford College discovered that a Google Group email list that was intended to be private was open to the entire Haverford community. Upon learning of the inadvertent misconfiguration, Haverford IT immediately re-set the permissions on the Group to prevent any continued unauthorized access, and ultimately shut the Group down to ensure the security of its vendor data. Haverford also reviewed the contents of the Google Group to determine whether any personal information was accessible. The ongoing investigation revealed that certain potentially accessible messages stored within the Google Group included PDF scans of vendor documents that included personal information. The potential unauthorized access to the Google Group was limited to the Haverford community. Haverford is unaware of any actual unauthorized access to the documents in the Google Group, or attempted misuse of the information.

2017 JAN 17 AM 11: 54

Notice to New Hampshire Resident

While the investigation is ongoing, Haverford has determined that the personal information of one (1) New Hampshire resident was stored and therefore potentially accessible on the inadvertently misconfigured Google Group. The personal information was the name, address, and social security number. On or about January 9, 2017, Haverford College is mailing written notice of this incident to the vendor whose personal information may have been affected by this incident in substantially the same form as the letter attached hereto as *Exhibit A*.

Other Steps Taken and To Be Taken

Haverford takes the security of its community members' information extremely seriously. In addition to the steps taken above, Haverford is providing its affected vendors notice of this incident and one year of complimentary credit monitoring and identity theft protection services through Experian, along with information on how to better protect against identity theft and fraud. Haverford has also implemented new procedures for the handling of vendor information to better protect personal information.

In addition to providing notice of this incident to your office, Haverford College is providing notice of this incident to other regulators and consumer reporting agencies where required.

Contact Information

Should you have any questions regarding this notification of other aspects of this event, please contact us at 267-930-4775.

Very truly yours,



Claudia McCarron of
MULLEN COUGHLIN LLC

CDM:hp
Enclosure

Exhibit A

[HAVERFORD COLLEGE LETTERHEAD]

[Date]

[Name]

[Street]

[City, State Zip Code]

Dear [Name]:

Haverford College (“Haverford”) is writing to alert you to an incident that may affect the security of your personal information. We have no evidence of actual unauthorized access to this personal information, however, in an abundance of caution, we are providing this notice to ensure that you are aware of the incident so that you may take steps to protect your information should you feel it is appropriate to do so.

What Happened? On August 2, 2016, Haverford College discovered that a Google Group email list that was intended to be private was open to the entire Haverford community. Haverford IT immediately secured access to the group to prevent continuing unauthorized access. An investigation revealed that certain potentially accessible messages stored within the Google Group included PDF scans of vendor documents that included personal information. The potential unauthorized access to the Google Group was limited to the Haverford community.

What Information Was Involved? While Haverford’s investigation is ongoing, Haverford has determined that there was a misconfiguration in a Google Group site that allowed unauthorized members of the Haverford community to access to certain files containing personal information related to individuals who have filed IRS form W-9s with the College. Information that may have been accessed included your name, address, and Social Security number. We have no evidence of actual unauthorized access to this information. Haverford is unaware of any actual or attempted misuse of that personal information.

What is Haverford Doing? Upon learning of the misconfigured privacy settings on the Google Group, Haverford immediately re-set the permissions on the Group and ultimately shut the Group down to ensure the security of our vendor data. We have conducted an investigation to ensure all affected individuals have been identified and provided notice of this incident. In addition to the steps taken above, we are providing you with additional information on how to better protect against identity theft and fraud. We are offering you access to 12 months of complimentary credit monitoring and identity restoration services with Experian ProtectMyID Alert. The enclosed Privacy Safeguards contains information on protecting against identity theft and fraud and instructions on how to enroll and receive the complimentary credit monitoring and identity restoration services.

What Can You Do? You can review the additional information included in the attached Privacy Safeguards on how to better protect against identity theft and fraud. You can also enroll to receive the complimentary access to 12 free months of credit monitoring and identity restoration services with Experian’s ProtectMyID Alert.

For More Information. Should you have any questions regarding this incident, please call (610) 896-1368 Monday through Friday, 9:00 a.m. – 4:00 p.m. EST.

We want to assure you that we continue to take appropriate actions to protect the privacy and security of your information.

Sincerely,

Megan Fitch
Chief Information Officer

PRIVACY SAFEGUARDS

To help detect the possible misuse of your information, we are offering you 12 months of credit monitoring and identity restoration services with Experian's ProtectMyID Alert at no cost to you.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: January 1, 2018** (Your code will not work after this date.)
2. Visit the **ProtectMyID Web Site to enroll: www.protectmyid.com/alert**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call (877) 297-7780 and provide engagement #: **PC105779**.

Additional details regarding your 12-MONTH ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
 - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian credit report.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
 - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, 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 877-297-7780.

You may take action directly to protect against possible identity theft or financial loss. 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

* 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.

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

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

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
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, list 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
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents please call
1-800-349-9960)
www.equifax.com/help/credit-freeze/en_cp

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

TransUnion
PO Box 2000
Chester, PA 19022-2000
www.transunion.com/securityfreeze
1-888-909-8872

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/idtheft, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Rhode Island residents, the

Attorney General's office can be contacted at <http://www.riag.ri.gov/index.php>, consumers@riag.ri.gov or (401) 274-4400.