LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS AT LAW

550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

JAMES E. PRENDERGAST
DIRECT DIAL: 215.977.4058
JIM.PRENDERGAST@LEWISBRISBOIS.COM

June 3, 2016

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 Attorney General Foster:

We represent Bucknell University, 701 Moore Ave, Lewisburg, PA 17837 ("Bucknell"), and are writing to notify your office of an incident that may affect the security of personal information relating to twenty-two (22) New Hampshire residents. By providing this notice, Bucknell does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction, or the applicability of the New Hampshire data event notification statute.

Nature of the Data Event

Bucknell University faculty and staff are provided with an internal electronic document storage application called Netspace. Within Netspace, certain folders are accessible to all individuals with both University login credentials and an additional level of authorization. As part of Bucknell's ongoing electronic security efforts, it deployed a tool to scan those Netspace folders in order to identify any sensitive data being stored there. On or around March 31, 2016 and April 11, 2016, Bucknell identified sensitive data elements located in a limited number of those Netspace folders. The data was immediately moved to a secure location and Bucknell began an investigation to determine whether any sensitive information was subject to unauthorized access or acquisition.

Bucknell was not able to determine when the information was placed in those Netspace folders, but was able to confirm that the information was **not** accessible from the web or by individuals who do not possess the login credentials described above. Bucknell also confirmed that to find the information, one would need to intentionally navigate to a particular faculty or staff member's

profile and access the specific folder containing that information. While Bucknell does not have any evidence suggesting that anyone improperly accessed the data, Bucknell determined on May 10, 2016 that it cannot definitively rule out access by unauthorized persons within the Bucknell community.

Notice to New Hampshire Residents

Notice was provided to twenty-two (22) of New Hampshire residents on June 3, 2016. Notice was provided in substantially the same format as the letter attached hereto as **Exhibit A.**

Other Steps Taken and To Be Taken

Upon discovering this incident, the information was immediately moved to a secure location. Bucknell hired nationally recognized forensic consultants to investigate whether any of the information was subject to unauthorized access or acquisition. After an extensive investigation, Bucknell found no evidence suggesting that anyone improperly accessed or acquired the information. However, because access could not be definitively ruled out, notice was provided.

Additionally, Bucknell is providing potentially affected individuals with one year of free credit monitoring and identify theft assistance through Experian. Bucknell is also reviewing its policies and procedures relating to data privacy and is taking steps to further educate its staff on appropriate storage of sensitive information. Bucknell will continue to deploy its scanning tool to ensure no information is placed on non-private Netspace folders.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-977-4058.

Very truly yours,

James E. Prendergast of
LEWIS BRISBOIS BISGAARD & SMITH LLP

JEP:ncl
Enclosure

EXHIBIT A

Bucknell
UNIVERSITY

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<First Name>><<Last Name>>
<<Address>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name>>:

I am writing on behalf of Bucknell University to notify you of a data event involving your personal information, as discussed further below. We are not aware of any actual or attempted misuse of your information, but we are sending this notice to you to let you know what steps we have taken to protect your information, to offer you access to complimentary credit monitoring and identity restoration services, and to provide you with information about additional ways to protect your identity should you wish to do so.

What Happened? Bucknell University faculty and staff are provided with an internal electronic document storage application called Netspace. Within Netspace, certain folders are accessible to all individuals with both University login credentials and an additional level of authorization. As part of our ongoing electronic security efforts, we use a tool called Identity Finder to scan those Netspace folders in order to identify any sensitive data being stored there. On or around March 31, 2016 and April 11, 2016, we identified sensitive data elements located in a limited number of those Netspace folders. The data was immediately moved to a secure location and we began an investigation to determine whether any sensitive information was subject to unauthorized access. We were not able to determine when the information was placed in those Netspace folders, but were able to confirm that the information was **not** accessible from the web or by individuals who do not possess the login credentials described above. We also confirmed that to find the information, one would need to intentionally navigate to a particular faculty or staff member's profile and access the specific folder containing that information. While we do not have any information suggesting that anyone improperly accessed your information, we cannot definitively rule out access by unauthorized persons within the Bucknell community.

What Information Was Involved? While there is no indication that any unauthorized individual took or viewed any of your information, your name, <<medical information, insurance information, credit card information and Social Security number>> were in one or more of the folders described above.

What We Are Doing. Bucknell University places the utmost value on the safety and security of its community members, including the security of their personal information. We assure you that Bucknell is taking steps to ensure your information is protected. We conduct regular Identity Finder scans consistent with best practices in information security, and are taking steps to help prevent a similar incident from occurring in the future. In addition, we are providing you with access to one year of credit monitoring and identity restoration services with Experian at no charge. The enclosed *Other Important Information* sheet contains instructions for enrolling in the credit monitoring and identity restoration services, as well as information on protecting yourself against identity theft and fraud.

What You Can Do. We encourage you to review the enclosed *Other Important Information* sheet and to take advantage of the complimentary identity monitoring and restoration services. You can contact us with questions regarding this incident by email at datasecurity@bucknell.edu, or by telephone at 570-577-7981. Voicemail messages left at that number will be returned Monday through Friday, 8:30 AM to 4:30 PM Eastern Time.

We sincerely apologize for this unfortunate incident and any inconvenience it may cause.

Sincerely,

Param Bedi

Param Bedi
Vice President for Library & Information Technology

OTHER IMPORTANT INFORMATION

To help protect your identity, we are offering a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. 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 ProtectMyID Now in Three Easy Steps

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

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: **<<engagement number>>**.

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, Equifax® and TransUnion® credit reports.
- **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[1]:** 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 877-288-8057.

We encourage you to remain vigilant against incidents of identity theft and financial loss by reviewing your account statements and monitoring your credit reports for suspicious activity. Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

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

At no charge, you can also have these credit bureaus place a "fraud alert" on your credit file. A "fraud alert" will tell creditors to take additional steps to verify your identity prior to granting credit in your name; however, because it tells creditors to follow certain procedures to protect you, the fraud alert may also delay your ability to obtain credit while the credit bureaus verify your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your files. You may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on your credit report.

[1] 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.

You can also place a "security freeze" on your credit file that prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. Again, doing so may delay, interfere with, or prevent the timely approval of any requests for new credit. If you have been a victim of identity theft and provide the credit reporting agency with a valid police report, the credit reporting agency cannot charge to place, lift or remove a security freeze. In all other cases, a credit agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. If you incur a cost to place a security freeze, please let us know. You must contact each of the credit reporting agencies separately to place a security freeze on your credit file:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents 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 Security Freeze
P.O. Box 2000
Chester, PA 19022-2000
888-909-8872
www.transunion.com/
securityfreeze

You can further educate yourself regarding identity theft, fraud alerts, security freezes, 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); and TTY: 1-866-653-4261. 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. You should report known or suspected identity theft or fraud to law enforcement, the FTC, and your state Attorney General.