



Bucknell University  
One Dent Drive  
Lewisburg, Pennsylvania 17837

**Bucknell**  
UNIVERSITY

[Date]

[First Name] [Last Name]  
[Address]  
[City] [State] [Zip]

Re: Notice of Data Event

Dear [First Name] [Last 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 this 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 academic and administrative departments maintain departmental webpages. Information for those webpages is stored in what are known as departmental webspaces. As part of our ongoing electronic security efforts, we use a tool called Identity Finder to scan certain University systems in order to identify any sensitive data being stored there. During a May 9, 2016 scan, we identified sensitive data elements, specifically social security numbers, located in a database stored in the pre-med program webpage. Because the data elements were stored in the webpage, they were accessible via the internet. We immediately moved the data to a secure location and began an investigation. We discovered that the database contained the social security numbers of a small number of former Bucknell University students. We believe that the information was made accessible sometime in or prior to February 2009. We found no evidence that any unauthorized person accessed or acquired this information, and we did not find any evidence that this information was cached or stored anywhere else online. Our investigation disclosed that in order to find the information, an individual would have had to type in a specific, lengthy URL assigned to the database. One could not access the database by simply searching for it using a search engine. Likewise, the database was not visible on or accessible via a link on the pre-med website. While we do not have any information suggesting that anyone improperly accessed the database, including your social security number, we cannot definitively rule out access by unauthorized persons, and, out of an abundance of caution, we are providing this notice to you.

***What Information Was Involved?*** While there is no indication that any unauthorized individual took or viewed any of your information, your name and Social Security number were included in the database.

***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 (1) year of credit monitoring

and identity restoration services with Experian at no charge to you. This coverage comes with fraud resolution support extending beyond the first year of monitoring. The enclosed *Other Important Information* sheet contains instructions for enrolling in the identity monitoring and 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 credit monitoring and identity restoration services.

***For More Information.*** You can contact us with questions regarding this incident by email at [datasecurity@bucknell.edu](mailto:datasecurity@bucknell.edu), or by telephone at 570-577-7981. Voicemail messages left at that number will be returned Monday through Friday, 8:00 AM to 4:0 PM Eastern Time.

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

Sincerely,

A handwritten signature in cursive script that reads "Param Bedi". The signature is written in black ink and is underlined with a single horizontal stroke.

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: **09/24/2016** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: [www.protectmyid.com/redeem](http://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 #: **PC102258**

### 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<sup>1</sup>:** 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,

---

<sup>1</sup> 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.

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  
P.O. Box 105069  
Atlanta, GA 30348  
800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19022-2000  
800-680-7289  
[www.transunion.com](http://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.

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](http://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](http://www.experian.com/freeze/center.html)

TransUnion Security Freeze  
P.O. Box 2000  
Chester, PA 19022-2000  
888-909-8872  
[www.transunion.com/securityfreeze](http://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](http://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](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). You should report known or suspected identity theft or fraud to law enforcement, the FTC, and your state Attorney General.