CONS.

PENNSTATE

David W. Dulabon
Associate General Counsel

Office of General Counsel
The Pennsylvania State University
227 West Beaver Avenue, Suite 507
State College, PA 16801

Tel: 814-865-0551
Fax: 814-863-8469
dwd117@psu.edu
http://ogc.psu.edu

May 18, 2015

VIA USPS FIRST CLASS MAIL

Office of the Attorney General
New Hampshire Department of Justice
Attn: Data Security Breach
33 Capitol Street
Concord, NH 03301

Subject: **Notification of Security Incident Pursuant to N.H. Rev. Stat. § 359-C:19 *et seq.***

To whom it may concern:

I am writing to notify you of a recent security incident at The Pennsylvania State University ("Penn State" or the "University").

In late November 2014, the Federal Bureau of Investigation ("FBI") provided a victim notification report to Penn State relating to suspicious cyber activity directed at certain systems and computers in the College of Engineering (the "College"). Penn State immediately launched a comprehensive internal investigation into the FBI's report and retained leading third-party computer forensics experts to assist in the investigation. By December 2014, the University was advised that several systems and computers in the College were the targets of highly sophisticated cyber-attacks, often referred to as an Advanced Persistent Threat. In this situation, there are indicators that suggest that a system or computer within the College may have been attacked as early as September 2012. At this time, we have no indication that personally identifiable information was taken during this initial attack.

The University and its forensic experts have since conducted a thorough analysis of the College of Engineering's computer network to determine the full scope of the security breach and have taken steps to restore the integrity of the College's systems. Based on further investigation into the attacks, we learned that personally identifiable information was contained on a system or computer within the College that may have been compromised in or around April 2014. As part of our investigation, Penn State conducted a comprehensive scan of the computers and systems for personally identifiable information, which ultimately involved 17,933 individuals. It is Penn State's understanding that 46 of these individuals are New Hampshire residents.

We have no indication that the personal information discovered on the systems and computers was specifically acquired or misused by unauthorized individuals. However, out of an abundance of caution, the University is notifying 17,933 individuals (including the 46 New Hampshire residents) of this incident by U.S. first class mail on May 19, 2015. A copy of the University's May 19, 2015 letter is attached as **Exhibit A**. The University also alerted all three major credit reporting agencies of this incident. Copies of the letters sent to the credit reporting agencies are attached as **Exhibit B.**

Since the incident, Penn State and its forensic experts have taken significant steps to fortify the College's cyber-security defenses. These measures will continue to provide the University with a greater capability to prevent, detect and respond to cyber-security issues.

If you have any additional questions about this incident, please call me at your earliest convenience at (814) 865-0551.

Very truly yours,

David W. Dulabon

David W. Dulabon
Associate General Counsel

Enclosures

EXHIBIT A

PENNSTATE

College of Engineering
The Pennsylvania State University
101 Hammond Building
University Park, PA 16802-1400

Anthony Atchley
Senior Associate Dean

May 19, 2015

##A8595-L01-0123456 T-0001 **********3-DIGIT 159
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A Sample:

I am writing to inform you of an incident involving The Pennsylvania State University's College of Engineering computer systems that may affect the confidentiality of your personally identifiable information. We have confirmed that a file or document containing your [Social Security Number, Driver's License Number, Bank Account Number and Credit Card Number] resided on a compromised system or computer within the College. Although Penn State is unaware of any attempted or actual misuse of your personal information, out of an abundance of caution, we are providing you notice of this incident, offering you free credit monitoring for one year, and advising you of potential steps you may wish to take.

What happened:

In late November 2014, the Federal Bureau of Investigation provided a victim notification report to Penn State relating to suspicious cyber activity directed at certain systems and computers in the College of Engineering. Penn State immediately launched a comprehensive internal investigation into the FBI's report and retained leading third-party computer forensic experts to assist in the investigation.

By December 2014, the University was advised that several systems and computers in the College were the targets of highly sophisticated cyber-attacks, often referred to as an Advanced Persistent Threat. In such an attack, the intruders orchestrate covert targeted attacks to gain access to a system and then employ sophisticated evasion techniques to remain undetected, sometimes for years. In this situation, there are indicators that suggest that a system or computer within the College may have been attacked as early as September 2012, and the intruders used sophisticated techniques to remain undetected. At this time, we have no indication that personally identifiable information was taken during this initial attack.

The University and its forensic experts have since conducted a thorough analysis of the College of Engineering's computer network to determine the full scope of the security breach and have taken steps to restore the integrity of the College's systems. Based on our further investigation into the attacks, we learned that personally identifiable information was contained on a system or computer within the College that may have been compromised in or around April 2014. As part of our investigation, we conducted a comprehensive scan of the computers and systems at issue for personally identifiable information. We recently completed our scan and analysis, and although we have no indication that your personal information was specifically acquired or misused by unauthorized individuals, we did learn that your personal information resided on a compromised system or computer within the College. Penn State feels it is important to bring this incident to your attention and to advise you of the steps being taken by the University to assist you. We would also like to recommend steps you can take to further protect yourself and provide you with contact information if you have further questions.

0123456

What we are doing to protect your information:

To help detect any possible misuse of your personal information, we are offering you access to a complimentary one-year membership to Experian's® ProtectMyID® Elite. Experian is the largest credit bureau in the United States, and the ProtectMyID Elite Service helps detect possible misuse of your personal information, provides you with superior identity protection support that is focused on immediate identification and resolution of identity theft, and provides free fraud resolution and identity protection for one-year. Please note you must activate this membership by **May 8, 2016**, which will then continue for 12 full months from your enrollment date.

To start monitoring your personal information, please follow the steps below:
Visit www.protectmyid.com/protect
Provide your activation code: **ABCDEFGHIJKL**

We encourage you to take advantage of this service and to activate the fraud detection tools available through ProtectMyID Elite. Please note that a credit card is **not** required for enrollment.

If you have questions or need an alternative to enrolling online, please call Experian at (866) 751-1324 and provide Engagement #: [redacted]

Once you enroll in ProtectMyID you will have access to the following tools

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors the Experian file for indicators of fraud.
- **Internet Scan:** Alerts you if your information is found on sites containing compromised data.
- **Address Change Alerts:** Alerts you of changes to your mailing address
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE:** You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** Get help replacing credit, debit, and medical insurance cards.

Once you have completed enrollment in ProtectMyID, you can receive alerts on your mobile phone by downloading the BillGuard mobile app for FREE. Use your ProtectMyID membership login credentials to sign in to the app in order to access - in one place - both your ProtectMyID alerts and BillGuard features, including monitoring against fraud on your current credit and debit card accounts. Visit protectmyid.com/billguard to learn more.

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 (866) 751-1324.

What you can do to further 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 the final page of this letter for those additional actions to help reduce your chances of identity theft.

We regret any concern or inconvenience. We make substantial efforts to protect sensitive information, but no organization is completely immune from malicious acts. We encourage you to take advantage of the free identity theft protection offered by Penn State. If you have any questions about this incident, please contact our call center toll-free at [redacted] Monday through Friday, 9 a.m. to 7 p.m. Eastern Time (closed on U.S. observed holidays). Please be prepared to provide the following ten-digit number when calling: [redacted]

Sincerely,

Anthony Atchley
Senior Associate Dean, College of Engineering

Case # IR-6057

0123456

A8595-L01

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

⇒ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An **initial 90 day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should takes steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

⇒ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

⇒ ORDER YOUR FREE ANNUAL CREDIT REPORTS

Visit www.annualcreditreport.com or call 877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

⇒ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

⇒ USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with the Federal Trade Commission (FTC), your State's Attorney General, or your local police and contact a credit reporting company.

⇒ OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.
- The Federal Trade Commission (600 Pennsylvania Avenue, NW, Washington, D.C. 20580) has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft.
- Many State Attorney General offices additionally provide information about protecting your identity on their websites.

EXHIBIT B

PENNSTATE

Office of Ethics and Compliance

The Pennsylvania State University
120 South Burrowes Street
State College, PA 16801

Phone: 814-863-5915
Fax: 814-863-2174

May 15, 2015

Equifax Information Services, LLC
P.O. BOX 105788
Atlanta GA 30348

Re: The Pennsylvania State University

To Whom It May Concern:

This letter is to advise you that approximately 17,933 individuals will be notified on May 19, 2015 by U.S. Mail of a security breach involving several systems and computers in the College of Engineering that was caused by two highly sophisticated cyber-attacks. The files and documents discovered on the systems and computers included full names and social security numbers, credit card numbers, bank account numbers and/or driver's license numbers.

Please feel free to contact me should you have any questions. I can be reached via telephone at (814) 863-5915.

Best regards,

Holly M. Swires
Privacy Officer

PENNSTATE

Office of Ethics and Compliance

The Pennsylvania State University
120 South Burrowes Street
State College, PA 16801

814-863-5915
Fax: 814-863-2174

May 15, 2015

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000

Re: The Pennsylvania State University

To Whom It May Concern:

This letter is to advise you that approximately 17,933 individuals will be notified on May 19, 2015 by U.S. Mail of a security breach involving several systems and computers in the College of Engineering that was caused by two highly sophisticated cyber-attacks. The files and documents discovered on the systems and computers included full names and social security numbers, credit card numbers, bank account numbers and/or driver's license numbers.

Please feel free to contact me should you have any questions. I can be reached via telephone at (814) 863-5915.

Best regards,

Holly M. Swires
Privacy Officer

PENNSTATE

Office of Ethics and Compliance

The Pennsylvania State University
120 South Burrowes Street
State College, PA 16801

814-863-5915
Fax: 814-863-2174

May 15, 2015

Experian
P.O. Box 9554
Allen TX 75013

Re: The Pennsylvania State University

To Whom It May Concern:

This letter is to advise you that approximately 17,933 individuals will be notified on May 19, 2015 by U.S. Mail of a security breach involving several systems and computers in the College of Engineering that was caused by two highly sophisticated cyber-attacks. The files and documents discovered on the systems and computers included full names and social security numbers, credit card numbers, bank account numbers and/or driver's license numbers.

Please feel free to contact me should you have any questions. I can be reached via telephone at (814) 863-5915.

Best regards,

Holly M. Swires
Privacy Officer