

PENNSSTATE



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

STATE OF NH
DEPT OF JUSTICE
2016 MAY 31 AM 11:53

May 24, 2016

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").

On April 13, 2016, Penn State's Office of Student Affairs received notification that a student organization's (the Undergraduate Law Society's) website contained a historical document containing Social Security Numbers (SSN's). The Penn State Office of Student Affairs immediately moved the student organization's website offline upon receiving report of the incident and alerted the University's Office of Information Security for further investigation.

Upon further investigation, the University confirmed that the historical document appearing on the student organization's website was an Excel file that included an SSN column and a date of birth column, both of which were hidden from view as presented on the website. The Excel file, however, could be manipulated in a way where the SSN's and the dates of birth potentially could have been exposed if those particular columns were "unhidden" in the Excel format. It is the University's understanding that the student organization last modified this Excel file in 2006.

Penn State conducted a careful review of this Excel spreadsheet and determined that 379 unique names and SSN's were contained in the hidden SSN column. Of the 379 individuals appearing on this Excel spreadsheet, it is Penn State's understanding that three (3) of them are New Hampshire residents.

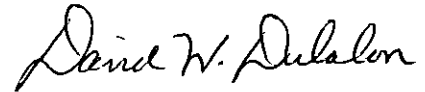
Pursuant to well-established University Policy, student organizations themselves (and not the University) are responsible for the content of their websites. While we have no indication that the personal information discovered was acquired or misused by unauthorized individuals,

out of an abundance of caution and in light of the fact that the Undergraduate Law Society is now defunct, the University is notifying 379 individuals (including the three (3) New Hampshire residents) of this incident by U.S. first class mail on May 25, 2016. A copy of the University's May 25, 2016 letter is attached as **Exhibit A**.

Since the incident, the University is working on educating student managed clubs and organizations about the importance of safeguarding their members' personally identifiable information (PII) and remediating historical PII. Penn State also is in the process of helping student clubs and organizations better manage their websites, including utilizing the University's Identity Finder software to scan for any inadvertent PII. The University also is offering the three (3) New Hampshire residents potentially impacted by this incident **one year** of free credit monitoring.

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

Very truly yours,

A handwritten signature in cursive script that reads "David W. Dulabon".

David W. Dulabon
Associate General Counsel

Enclosure

EXHIBIT A



PennState

Privacy Office

333 James M. Elliott Bldg.
120 S. Burrowes St.
State College, PA 16801

Phone: 814-863-8918
Fax: 814-863-2174

May 25, 2016

[NAME & Address OF RECIPIENT]

Dear [NAME OF RECIPIENT]

I am writing to inform you of an incident that was recently discovered that may affect the confidentiality of your personally identifiable information ("PII"). We have confirmed that a historical document containing your PII resided on web space assigned to a now defunct student organization. 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:

On April 13, 2016, Penn State's Office of Student Affairs received notification that a student organization's (the Undergraduate Law Society's) website contained a historical document containing Social Security Numbers (SSN's). The Penn State Office of Student Affairs immediately moved the student organization's website offline upon receiving report of the incident and alerted the University's Office of Information Security for further investigation.

Upon further investigation, the University confirmed that the historical document appearing on the Undergraduate Law Society's website was an Excel file that included an SSN column and a date of birth column, both of which were hidden from view as presented on the website. The Excel file, however, could be manipulated in a way where the SSN's and dates of birth potentially could have been exposed if those particular columns were "unhidden" in the Excel format. It is the University's understanding that the student organization last modified this Excel file in 2006.

While we have no indication that the personal information discovered in this historical file appearing on the student organization's website was specifically acquired or accessed by unauthorized individuals, Penn State feels it is important to bring this to your attention and to advise you of the steps being taken by the University to assist you.

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 August 31, 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: [code]

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.


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 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 Holly Swires at (814) 863-5915, Monday through Friday, 7:30 a.m. to 4:30 p.m.

Sincerely,



Holly M. Swires
Privacy Officer

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 take 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
P.O. Box 105788
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-680-7289
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

Remain vigilant and 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.
- For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us
- For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division Mall Service Center 9001, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov
- For residents of California: You may also obtain information on protection against identity theft from the California Office of Privacy Protection, www.privacy.ca.gov.
- Many State Attorney General Offices additionally provide information about protecting your identity on their websites.