



MULLEN  
COUGHLIN<sub>LLC</sub>

Sian Schafle  
Office: 267-930-4799  
Fax: 267-930-4771  
Email: [sschafle@mullen.law](mailto:sschafle@mullen.law)

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

April 18, 2017

**VIA E-MAIL AND U.S. MAIL**

Office of the Attorney General  
1125 Washington Street SE  
P.O. Box 40100  
Olympia, WA 98504-0100  
E-Mail: [securitybreach@atg.wa.gov](mailto:securitybreach@atg.wa.gov)

**Re: Notice of Data Security Incident**

Dear Sir or Madam:

We represent Pacific Lutheran University (“PLU”), 12180 Park Avenue S, Tacoma, Washington 98447, and are writing to notify you of a recent incident that may affect the security of the personal information of eight hundred thirteen (813) Washington residents. The investigation into this incident is ongoing and will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, PLU does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

**Nature of the Data Security Incident**

On January 26, 2017, PLU became aware that certain employees, students, and other affiliates of PLU received a phishing email via their PLU email accounts, purporting to be from the university’s President. The phishing email contained a link that would redirect anyone who clicked on it to a website that requested the user’s PLU email log-in credentials. Upon discovering this issue, PLU immediately launched an investigation and began working with an outside computer forensics expert to confirm the security of our systems and to determine whether protected information was potentially impacted as a result of this incident. Through PLU’s investigation, it determined that, as a result of the phishing email attacks, an unauthorized individual or individuals may have accessed personally identifiable information (“PII”) contained within certain PLU employee email accounts and, separately, certain PLU employees’ Form W-2s contained within those employees’ Banner accounts. This potential unauthorized activity is believed to have occurred between January 23, 2017 and February 22, 2017.

Based upon this finding, an intensive forensic review of the impacted PLU email accounts’ contents was performed to identify all individuals for whom PII was contained within the impacted PLU

email accounts. The large volume and variety of documents in need of review required a combination of automated forensic tools and manual document review by a forensics expert to check the data contents for the presence of PII. Once all potentially affected individuals were identified, PLU engaged in an additional process of identifying and confirming address information for the affected population, which involved both a review of PLU's internal records and National Change of Address ("NCOA") database address verification provided by an outside vendor.

The types of PII relating to Washington residents determined to be stored within the impacted PLU email accounts were not identical for every potentially affected individual, and they included the following: name, Social Security number, date of birth, driver's license number, financial account information, and credit/debit card information.

A review of the impacted employee Banner accounts was also performed to determine what employee PII may have been stored within those accounts and, therefore, potentially impacted by this incident. PLU confirmed certain Benner accounts contained the Form W-2 of the employee to whom each account was assigned. A Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information.

### **Notice to Washington Residents**

On April 18, 2017, PLU mailed written notice of this incident to potentially affected individuals, including eight hundred thirteen (813) Washington residents. Such notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

### **Other Steps Taken**

PLU is offering potentially affected individuals complimentary access to 12 months of free credit monitoring and identity protection services with Kroll, as well as information on how to protect against identity theft and fraud, including information on how to contact the Federal Trade Commission, the state attorney general, and law enforcement to report any attempted or actual identity theft and fraud. In addition to providing notice of this incident to you, PLU reported this incident to the FBI and is providing written notice of this incident to other state regulators where required.

Since learning of this incident, PLU has contacted impacted PLU email account holders to encourage them to change their account passwords. PLU continues to review its information security practices in an effort to further enhance the security of its systems and better protect against future incidents of this kind.

Office of the Attorney General

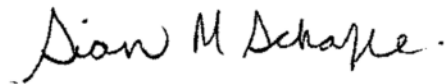
April 18, 2017

Page 3

### Contact Information

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me at (267) 930-4799.

Very Truly Yours,

A handwritten signature in black ink that reads "Sian M. Schafle." The signature is written in a cursive, flowing style.

Sian M. Schafle of  
MULLEN COUGHLIN LLC

SMS:atw

Enclosure

cc: Office of the Attorney General  
Consumer Protection Division  
800 5th Ave., Suite 2000  
Seattle, WA 98104-3188  
E-Mail: [securitybreach@atg.wa.gov](mailto:securitybreach@atg.wa.gov)

# **EXHIBIT A**



PACIFIC  
LUTHERAN  
UNIVERSITY

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<ZipCode>>

## Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

Pacific Lutheran University (“PLU”), is writing to notify you of a recent incident that may affect the security of your personal information. Although we are unaware of any actual or attempted misuse of your information, we are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect against identity theft and fraud should you feel it is appropriate to do so.

**What Happened?** On January 26, 2017, PLU became aware of a “phishing” email sent to certain PLU staff and student email accounts on January 23, 2017. That email was fraudulently written to appear as if it was sent by university President, Thomas Krise, and prompted recipients to enter their PLU email account username and password. Upon discovering this issue, PLU immediately launched an investigation and began working with an outside computer forensics expert to confirm the security of our systems and to determine whether protected information was potentially impacted as a result of this incident. It was determined that a number of PLU email accounts, **including yours**, were logged into by an unauthorized individual between January 23, 2017 and February 22, 2017, and that some of these email accounts contained personal information.

Our investigation further determined that the credentials used by the unauthorized individual to login to your PLU email account were identical to the credentials you use to access your PLU Banner account.

**What Information Was Involved?** Our investigation determined the following types of your information were stored within one or more affected email accounts: name, <<ClientDef1 (driver’s license number, state identification card number, Social Security number, financial account information, payment card number, student identification number, transcript, medical information, health insurance information, username/password, passport number, date of birth)>>.

**What We Are Doing.** At PLU we take your privacy and the security of the personal information within our care very seriously. We are taking steps to enhance data security protections to prevent similar incidents in the future. We reported this incident to the FBI and are also notifying certain government regulators about this incident.

We are providing you with information you may use to better protect against the potential misuse of your information. We have also secured the services of Kroll to provide identity monitoring at no cost to you for 1 year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. More detailed information on these services are included in the enclosed materials.

Visit [krollbreach.idMonitoringService.com](http://krollbreach.idMonitoringService.com) to activate and take advantage of your identity monitoring services.

*You have until July 21, 2017 to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605.

**What You Can Do.** You can enroll in the Kroll identity monitoring services. You can also review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*, which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft. Because your personal information may have been subject to unauthorized access, we encourage you to file your 2016 federal and state tax return as soon as possible if you have not already done so.

**For More Information:** We recognize that you may have questions that are not answered in this letter. If you have questions, please call 1-866-775-4209, Monday through Friday from 6:00 a.m. to 3:00 p.m. Pacific Time. Please have your membership number ready (included in the enrollment instructions above).

We sincerely regret any inconvenience this incident may cause. PLU remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

A handwritten signature in black ink, appearing to read "Susan J. Liden". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Susan J. Liden  
Director, Risk Management and Insurance

## Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to file your 2016 federal and state tax return as soon as possible, if you have not already done so. If you have not already filed, we encourage you to file IRS Form 14039 with your 2016 tax return. You can also contact the IRS at [www.irs.gov/Individuals/Identity-Protection](http://www.irs.gov/Individuals/Identity-Protection) for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit [www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft) for more information.

You should also look to the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each U.S. state's tax authority, visit <http://www.taxadmin.org/state-tax-agencies>.

In addition to enrolling to receive the services detailed above, you may take action directly to further 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 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](http://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](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 19016  
800-680-7289  
[www.transunion.com](http://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, lift 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)  
<https://www.freeze.equifax.com>

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  
P.O. Box 2000  
Chester, PA 19022-2000  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. 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](http://www.ftc.gov/idtheft), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. 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 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 at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, [www.ncdoj.gov](http://www.ncdoj.gov).



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services<sup>1</sup> from Kroll:

### **Credit Monitoring through TransUnion**

You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

### **Web Watcher**

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

### **Public Persona**

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

### **Quick Cash Scan**

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

### **\$1 Million Identity Fraud Loss Reimbursement**

Reimburses you for out-of-pocket expenses totaling up to \$1 million in legal costs for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.