

James J. Giszczak
Direct Dial: 248.220.1354
jgiszczak@mcdonaldhopkins.com

April 15, 2014

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Seattle University – Incident Notification

Dear Attorney General Delaney:

We represent Seattle University (the “University”) and are writing to notify you of a data privacy incident that may affect the security of personal information of one (1) New Hampshire resident. The University’s investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission. By providing this notice, the University does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On February 21, 2014, a Seattle University email account user initially brought a situation to the University’s attention. The University determined that a certain number of folders within the University’s Microsoft Exchange folder system contained incorrect permission settings. The settings made it possible for information in these folders to be viewed by unauthorized individuals if they had a Seattle University email account. Even then, an individual would have had to navigate through multiple folders to access the information.

Upon learning of the situation, the University immediately took steps to correct the permission settings, monitor the affected folders and commenced a thorough investigation. As part of the investigation, the University hired a nationally respected firm specializing in digital forensic analysis. Considerable time and effort was required to determine what and whose exact information may have been affected.

The affected New Hampshire resident had applied for a student worker position in the University’s Department of Public Safety and Transportation between 2010 and 2014. The Application for such position included the resident’s full name and Social Security number. The Application has been revised to no longer collect this information.

Attorney General Michael A. Delaney
April 15, 2014
Page 2

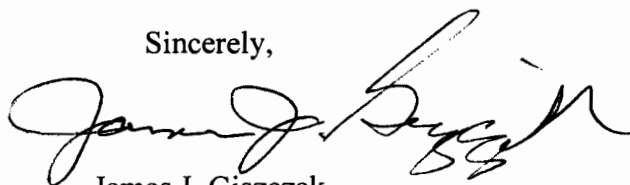
Although the University is aware that one user viewed information in these folders and subsequently reported the issue to administration officials, the University is neither aware of any unauthorized use of personally identifiable information nor does it have any indication to date that any identity fraud, theft, misuse or other harmful activity has occurred as a result of this situation. Nevertheless, we wanted to make you (and the affected resident) aware of the incident and explain the steps the University is taking to safeguard the resident against identity fraud.

The University mailed a notification letter to the New Hampshire resident on April 15, 2014, in substantially the same form as the letter attached hereto. The University has advised the resident to monitor all credit reports and financial statements for any suspicious activity. The University has offered a complimentary one-year membership in Experian's® ProtectMyID® to the affected resident. The University is also providing call center support for those affected. The University also advised the individuals affected to obtain a credit report and the process for placing a fraud alert on their credit files.

Maintaining the privacy of personal information is of the utmost importance to Seattle University. Significant investments have been made in recent years to upgrade the University's technology infrastructure to effectively support the work done at Seattle University and strengthen safeguards for protecting the information of its students, faculty and staff. The University is continuing its efforts to protect personal information and prevent this or a similar situation from happening again.

Should you have any questions regarding this notification or the incident, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,



James J. Giszczak

JJG/dap
Encl.



PO Box 6336
Portland, OR 97228-6336

**IMPORTANT INFORMATION
PLEASE READ CAREFULLY**

<<mail id>>
<<Name1>>
<<Name2>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>
<<Foreign Country>>

<<Date>>

Dear <FirstName> <LastName>.

Soon after learning of an internal data security situation in late February, Chuck Porter, Seattle University's Chief Information Officer, made me aware of the issue. Following a comprehensive investigation, we have now confirmed it involved your personally identifiable information (full name and Social Security number) maintained by the university and it was possible your information could have been viewed by others within the university community.

I hope you will accept my sincere apology. Protecting your personal information is one of our highest priorities.

Although I have been assured that no evidence has been uncovered to suggest any attempted or actual misuse of your information, you are being notified out of an abundance of caution and diligence. The personally identifiable information of 628 former and current students was viewable and, as a result, susceptible to unauthorized use.

We are sharing what we know with you now that we have completed a thorough investigation and been able to ascertain the facts, understand precisely who was affected and determine the extent of the information that was vulnerable. The investigation involved a digital forensics analysis and took several weeks to complete.

A Seattle University email account user initially brought the situation to our attention on February 21, 2014. We determined that a small number of folders within the university's Microsoft Exchange folder system contained incorrect permission settings. The settings made it possible for information in these folders to be viewed by unauthorized individuals if they had a Seattle University email account. Even then, an individual would have had to navigate through multiple folders to access the information. Upon learning of the situation, the Office of Information Technology (OIT) immediately took steps to correct the permission settings, monitor the affected folders and commence a thorough investigation.

As part of the investigation, OIT hired a nationally respected firm specializing in digital forensic analysis. Considerable time and effort was required to determine what and whose exact information may have been affected. We discovered that one of the affected folders contained your student application for employment with the Department of Public Safety and Transportation. As a result, the information in your application, including your full name and Social Security number, was viewable by university email account holders.

Although the university is aware that one user viewed information in these folders and subsequently reported the issue to administration officials, let me reiterate that we are neither aware of any unauthorized use of your personally identifiable information nor do we have any indication to date that any identity fraud, theft, misuse or other harmful activity has occurred as a result of this situation. Nevertheless, we believe it is important to make you aware of the issue and explain the steps we are taking to safeguard you against identity fraud and suggest steps that you should take as well.

To help protect your identity, we are offering you a complimentary one-year membership of Experian's® ProtectMyID® Alert. Please see the enclosed information regarding enrolling in this complimentary service, along with other preventive measures you can take, including placing a fraud alert and obtaining a free credit report.

If you have any further questions, please call the toll-free number we have set up to respond to questions at (877) 276-7349. Callers will need to use reference number: 46811. The hours are Monday through Friday, 6 a.m. to 6 p.m. Pacific Time. Additional information is available on the university's website at www.seattleu.edu/datasecurity.

Again, I deeply regret that your personal information was viewable. Significant investments have been made in recent years to upgrade our technology infrastructure to effectively support the work done at Seattle University and strengthen safeguards for protecting the information of our students, faculty and staff. Please know that we are continuing our efforts to protect your personal information and prevent this or a similar situation from happening again.

Sincerely,



Stephen V. Sundborg, S.J.

President

1. **Enrolling in Complimentary 12 Month Credit Monitoring**

Protecting your personal information is important to Seattle University. As a precautionary measure in response to the internal data security situation, we have arranged for you to enroll in Experian's® ProtectMyID® Alert for a one year period at no cost to you. Experian, the provider of the protection, is one of the three major nationwide credit reporting companies.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE that you enroll by **July 17, 2014**.
2. VISIT the ProtectMyID Web Site to enroll: www.protectmyid.com/redeem
3. PROVIDE your 9-character Activation Code: <XXXXXXXXXX>

If you have questions or need an alternative to enrolling online, please call 877-371-7902.

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 Identify 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:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of 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.)

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 877-371-7902.

2. **Placing a Fraud Alert**

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

TransUnion
Consumer Fraud Division
PO Box 6790
Fullerton, CA 92834-6790
www.transunion.com/fraud
1-800-680-7289

Experian
Consumer Fraud Division
PO Box 9554
Allen, TX 75013
www.experian.com
1-888-397-3742

Equifax
Consumer Fraud Division
PO Box 740256
Atlanta, GA 30374-0256
www.equifax.com
1-800-525-6285

3. **Obtaining a Free Credit Report**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit report online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338) or by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations.