McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

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

July 17, 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 security issue that may affect the personal information of nine (9) New Hampshire residents. 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 May 25, 2014, Seattle University's Chief Information Officer was made aware of an internal data security issue involving incorrect permission settings on an internal drive. The incorrect permission settings made it possible for individuals with a Seattle University computer account to view scanned checks stored on one of the internal drives, without proper authorization. The information includes scanned images of personal checks from donors to the University.

Upon learning of the situation, the University immediately took steps to correct the permission settings and commenced a thorough investigation. As part of the investigation, the University hired attorneys to conduct a manual review of the scanned checks to determine who may be affected and what information was viewable. After completing the manual review, on June 20, 2014, Seattle University learned that your residents were among the group of affected individuals.

The manual review confirmed that the residents' names, bank routing numbers and checking account numbers were viewable as a result of this incident. No PINS, security codes, access codes, or passwords were included with the checks. In addition, no other donor

information, including Social Security numbers and credit/debit card numbers, was susceptible to unauthorized viewing.

Although the University has been assured that there is no evidence to suggest any attempted or actual misuse of the information on the personal checks, the University wanted to make you (and the affected residents) aware of the incident and explain the steps the University is taking to safeguard the residents.

Seattle University is providing the New Hampshire residents with written notice of this issue, in substantially the same form as the letter attached hereto, with mailing commencing on July 17, 2014. The University has advised the residents to remain vigilant in reviewing their financial account statements for fraudulent or irregular activity on a regular basis. The University is also providing dedicated call center support for those affected. The University has advised these individuals about the process for placing a fraud alert on their credit files and obtaining a free credit report. The residents have also been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission. Seattle University also recommended that the residents consider calling their banking institution to determine if they should change their bank account number.

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 it maintains. 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.

Return Mail Processing Center
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 <<NAME>>,

On May 25, 2014, our Chief Information Officer was made aware of an internal data security issue involving incorrect permission settings. The incorrect settings made it possible for individuals with a Seattle University computer account to view certain confidential information online without proper authorization. The information included scanned images of some personal checks from donors to the University. Following a comprehensive investigation, we discovered that your personal check, made payable to the University, was among the scanned images that were viewable by University computer account holders.

No other donor information, including your Social Security number or credit/debit card number, was susceptible to unauthorized viewing. The scanned images were not exposed in any way to the general public or Internet at large. Immediate steps were taken to correct the permission settings and additional safeguards have since been put in place to prevent this or a similar situation from happening again.

Although I have been assured that there is no evidence to suggest any attempted or actual misuse of the information on your personal check (which contained your name, bank routing number, and checking account number), we are notifying you out of an abundance of caution.

I hope you will accept my sincere apology. Donor generosity represents an important vote of confidence in Seattle University's mission and work. Protecting your personal information is one of our highest priorities.

Please see the enclosed information regarding preventive measures you can take to protect and monitor your personal information, including placing a fraud alert and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis. Finally, you might want to consider calling your banking institution to determine if you should change your bank account number.

If you have any further questions, or would like information about the specifics of the exposed check, please call the toll-free number we have set up to respond to questions at (877) 276-7335. The hours are Monday through Friday, 6 a.m. to 6 p.m. Pacific Time.

Sincerely,

Michael Podlin
Vice President University Advancement

- ADDITIONAL INFORMATION -

1. Placing a 90-Day Fraud Alert on Your Credit File.

You might want to 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 in your name, increase the credit limit on an existing account, or provide a new card on an existing account. 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
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

2. Placing a Security Freeze on Your Credit File.

In addition, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies.

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 Federal Trade Commission, Consumer Response Center, 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. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

4. Contacting Your Banking Institution.

Since your banking information was involved in this incident, we advise you to call your banking institution to determine if you should change your bank account number.