VedderPrice

Chicago
New York
Washington, DC
London
San Francisco
Los Angeles
Singapore
vedderprice.com

June 29, 2018

Blaine C. Kimrey
Shareholder
+1 312 609 7865
bkimrey@vedderprice.com

VIA E-MAIL (SECURITYBREACH@ATG.WA.GOV)
Washington Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Notice of Data Security Incident

Dear Sir or Madam:

I represent Northwest University ("Northwest"). I'm writing to inform you of a recent data security incident at Northwest that may have impacted the security of certain personal information of 1,434 Washington residents.

Background of the Incident

Northwest is a non-profit private Christian university located in Kirkland, Washington. Northwest offers more than 70 majors and academic programs and enrolls students from across the country and throughout the world.

On June 20, 2018, Northwest became aware that an unauthorized third party gained access to certain documents that may have contained personal information, including names, addresses, dates of birth, Social Security Numbers and/or protected health information. The unauthorized third party accessed these documents by accessing an employee's e-mail account and inbox.

At this time, Northwest has no evidence that any of Northwest's internal systems other than this individual employee's e-mail account have been compromised. We also have no evidence that the individual who accessed the account has downloaded or otherwise exfiltrated any data or has engaged in any form of identity theft.

Notice to Washington Residents

On 29, the affected residents were notified of the incident. Enclosed is a sample of the notification letter sent to the affected residents. Northwest has also arranged to offer one (1) year of complimentary credit monitoring and identity theft protection services through Experian to the affected residents. Additionally, Northwest has established a call center that the affected residents can contact, toll-free, to ask questions and to receive further information regarding the incident.

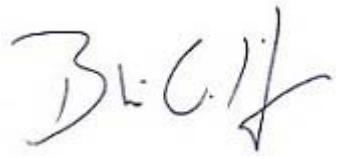
Other Steps Taken by Northwest University

Once Northwest was aware of the incident, Northwest promptly identified the attacker's means of access and implemented technical safeguards to ensure that the attacker's access was terminated. Northwest University also has retained a third-party forensics vendor to evaluate how the attack occurred, determine what information has been accessed, and confirm that the attacker's access has been terminated. Northwest can confirm that the attacker's access to the employee's e-mail account has been terminated and that Northwest has redoubled its efforts to ensure the confidentiality of account access credentials.

Contact Information

Please contact me if you have any questions or if I can provide you with any further information concerning this matter. Thank you.

Very truly yours,



Blaine C. Kimrey

Enclosure

Northwest
UNIVERSITY
5520 108th Ave NE
Kirkland, WA 98033

June 29, 2018

##D8502-L01-0123456 0001 00000001 **********9-OELZZ 123
SAMPLE A SAMPLE - NON-MA
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A Sample:

Northwest University values and respects your privacy, which is why we are writing to make you aware of a recent incident that may have involved your personal information.

What Happened

On June 20, 2018, Northwest University became aware that an unauthorized third party gained access to certain documents that may have contained your personal information. The unauthorized third party accessed these documents by accessing an employee's e-mail account and inbox.

At this time, we have no evidence that any of Northwest University's internal systems other than this individual employee's e-mail account have been compromised. We also have no evidence that the individual who accessed the account has downloaded or otherwise exfiltrated any data or has engaged in any form of identity theft, but out of an abundance of caution we are providing this notice to you.

What Information Was Involved

The information potentially at risk may include your name, address, date of birth, Social Security Number, bank account number, credit card number, and/or protected health information.

0123456

What We Are Doing

Investigation. Northwest University promptly identified the attacker's means of access and implemented technical safeguards to ensure that the attacker's access was terminated. Northwest University also has retained a third-party forensics vendor to evaluate how the attack occurred, determine what information has been accessed, and confirm that the attacker's access has been terminated.

D8502-L01

Mitigation. Northwest University has retained Experian to provide, at no cost to you, credit monitoring services. The details for opting in to these services are set forth below.

Protection Against Further Harm. The attacker's access to the employee's e-mail account has been terminated, and Northwest University has redoubled its efforts to ensure the confidentiality of account access credentials.

What You Can Do

Although we do not have any evidence that your information was misused as a result of this incident, you may be at risk. To help protect you, we have partnered with Experian to provide its IdentityWorks℠ product.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks℠ as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **October 31, 2018** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/3bcredit**
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332. Be prepared to provide engagement number **DB07452** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 12-MONTH EXPERIAN IDENTITYWORKS Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to 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 www.ExperianIDWorks.com/restoration for this information.

Remain vigilant for any unauthorized use of your information. We suggest that you monitor your credit reports, which you can obtain for free from the three credit reporting agencies listed below. If you suspect incidents of identity theft, you should notify local law enforcement and/or your state attorney general.

Equifax P.O. Box 105788 Atlanta, GA 30348 (800) 525-6285 www.equifax.com	Experian P.O. Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com	TransUnion Fraud Victim Asst. Div. P.O. Box 6790 Fullerton, CA 92834 (800) 680-7289 www.transunion.com

You may also want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least ninety (90) days. The alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at http://www.annualcreditreport.com.

For More Information

If you have questions or concerns, please contact our toll free number, (855) 776-8286, Monday through Friday, 6 a.m. to 6 p.m. Pacific Time, and Saturday through Sunday, 8 a.m. to 5 p.m. Pacific Time. Additionally, for more information about avoiding identity theft, you can contact the Federal Trade Commission at 600 Pennsylvania Ave. N.W., Washington, D.C. 20580, 1-877-ID-THEFT, consumer.ftc.gov. Residents of Maryland may also obtain information about avoiding identity theft from the Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. Residents of North Carolina may also obtain information about avoiding identity theft from the North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov. Residents of Oregon may also obtain information about avoiding identity theft from the Oregon Office of the Attorney General at 1162 Court St. NE, Salem, OR, 97301-4096, 1-877-877-9392, https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/.

Sincerely,

John Jordan
CFO
Northwest University

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (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