Angelina W. Freind
Office: (267) 930-4782
Fax: (267) 930-4771
Email: afreind@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

April 1, 2020

INTENDED FOR ADDRESSEE(S) ONLY

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent The Northshore Utility District ("Northshore") located at 6830 NE 185th St, Kenmore, Washington 98028, and are writing to notify your office of an incident that may affect the security of certain customer's personally identifiable information. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Northshore does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 12, 2020 a Northshore employee received an email that appeared to be from a legitimate King County, WA employee. It was discovered that the email contained a link that allowed unknown actors to temporarily gain access to the employee's email account. Northshore quickly launched an investigation and began working with computer forensic specialists to determine the full nature and scope of the activity. The investigation confirmed that one employee email account was accessed without authorization for a limited period of time on February 12, 2020.

However, the investigation was unable to determine what, if any, emails and attachments in the account were viewed by the unauthorized actor. Northshore undertook a comprehensive review of the contents of impacted email account to identify those who may have had personal information impacted as a result of this event. This review was completed on or about March 9, 2020. The personal information impacted by this event may include the following: name, Date of Birth, driver's license or state ID number, payment card information, financial account information, health insurance information, limited medical information, passport number, and Social Security number. There is no evidence this information was accessed by the unknown actor and Northshore is providing notice in an abundance of caution.

Notice to Washington Residents

On or about March 13, 2020, Northshore provided preliminary notice of this event to impacted current and former employees via email. A copy of the preliminary email communication is attached hereto as ***Exhibit* A**. On or about April 1, 2020 Northshore began mailing written notice of this incident to all affected individuals for whom it had sufficient address information, which includes approximately four hundred eighty-three (483) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

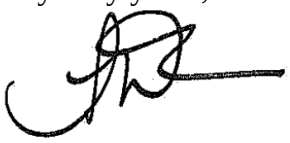
Upon discovering the event, Northshore moved quickly to investigate and respond to the incident, assess the security of Northshore's email environment, and notify potentially affected individuals. Northshore is providing individuals with information accessible within the account access to two (2) years of complimentary credit monitoring services through ID Experts. Northshore is also working to review existing policies and procedures.

Additionally, Northshore is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Northshore is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Northshore also reported this incident to Federal law enforcement and is cooperating as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4782.

Very truly yours,



Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/mef
Enclosure

c.c.: Office of the Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188
E-mail: securitybreach@atg.wa.gov
(via email)

EXHIBIT A

PRIVILEGED & CONFIDENTIAL
ATTORNEY CLIENT WORK PRODUCT

INDIVIDUAL ONLY

TO: Northshore Employees and Former Employees Impacted by February 2020 Event
RE: URGENT COMMUNICATION – Preliminary Notice of Data Incident

We've been diligently working to investigate an email phishing incident that recently impacted Northshore Utility District. As you may be aware, on or about February 12, 2020, one of our employees received an email from what appeared to be a legitimate King County email address. Unfortunately, the email contained a link that allowed unknown actors to temporarily gain access to the employee's email account for a limited period of time. We immediately began working with cybersecurity specialists to confirm the full nature and scope of the event and mitigate the impact of the attack. We also changed the credentials for the email account and implemented additional security measures to ensure the safety of our email environment.

The confidentiality, privacy, and security of our employee information is one of our highest priorities. While the investigation is ongoing, we felt it important to notify you about this incident and the steps we are taking to investigate and respond. Based on the findings of our investigation to date, we have reason to believe that certain elements of your personal information, such as your name, address, and Social Security number may have been contained in an email or attachment within the impacted email account, and may therefore have been accessible to the unauthorized actor. Here are some actions that we are taking and that we encourage you to take:

- Identity Protection. As a precaution, for those individuals affected by this incident, we arranged for identity theft protection services through ID Experts®, a data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

- ***We strongly encourage you to act to take advantage of these complimentary identity protection services as soon as possible.*** It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service. To enroll, please call 1-800-939-4170 or visit: https://app.myidcare.com/account-creation/protect, and enter Enrollment Code: NUD1BCSFAM24.

- Call Center for Employee Questions. We established a call center to answer common questions regarding this incident. ***Please note that the call center will be available Monday through Friday from 6 am - 6 pm Pacific Time. It is not available on Saturdays or Sundays.*** You may reach the call center toll free at 1-800-939-4170.

- Written Notification. You will receive a letter from the District in the next few weeks with additional information about the incident, the steps being taken in response, and steps you can take to further protect your personal information.

- Notice to Law Enforcement. We notified federal law enforcement of the incident and are cooperating with their investigation. We will also be notifying state Attorneys General, as required.

- Information Technology Systems Review. At this time, we do not believe that our IT systems were otherwise impacted by this attack. However, our IT team, with assistance from cybersecurity specialists, are assessing the security and soundness of our systems and determining how best to prevent these types of attacks in the future.

- Employee Training. Unfortunately, even the best technology cannot prevent all cyber-attacks, particularly email phishing scams. We will continue to provide, and improve upon, our information security awareness and training programs for all employees.

We apologize for any inconvenience this incident causes you. Please know that we are working diligently to investigate this event and to prevent similar incidents from occurring in the future. If you have any questions about the contents of this message or about the incident, please contact our call center toll free at 1-800-939-4170.

EXHIBIT B

C/O ID Experts
10300 SW Greenburg Rd., Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

April 1, 2020

RE: Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

The Northshore Utility District ("Northshore") writes to notify you of a recent incident that may affect the security of some of your personal information. We are providing you with details about the event, steps we are taking in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On February 12, 2020 a Northshore employee received an email that appeared to be from a legitimate King County email address. It was discovered that the email contained a link that allowed unknown actors to temporarily gain access to the employee's email account. Northshore quickly launched an investigation to determine the full nature and scope of the activity. With the assistance of leading computer forensics specialists, we learned that one employee email account was accessed without authorization for a limited period of time on February 12, 2020.

However, the investigation was unable to determine what, if any, emails and attachments in the account were viewed by the unauthorized actor. We immediately undertook a comprehensive review of the contents of impacted email account to identify those who may have personal information accessible within the impacted account. We completed this review on or about March 9, 2020 and determined that information related to you was present in the email account during the period of unauthorized access.

What Information Was Involved? Northshore's investigation confirmed the information present within the impacted email account at the time of the incident includes your name and <<variable data>>.

What We Are Doing. Information privacy and security are among our highest priorities. Northshore has security measures in place to protect information in our care. Upon learning of this incident, Northshore took steps to confirm and further strengthen the security of our systems, including our email accounts. As a precautionary matter, Northshore also notified law local and federal enforcement agencies, and continues to review its security policies and procedures as part of its ongoing commitment to information security.

In addition, we arranged for identity theft protection services through ID Experts®, a data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. Information on how to enroll in these services may be found in the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud."

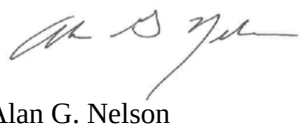
What You Can Do. You may review the information contained in the enclosed "Steps You Can Take to Protect Your Personal Information" for guidance on how to protect your personal information. You may also enroll to receive the identity and credit monitoring services we are making available to you as we are unable to enroll in these services on your behalf.

We encourage you to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and report any suspicious activity immediately to your insurance company, health care provider, or financial institution. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit 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.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, we established a dedicated assistance line at 1-800-939-4170, which can be reached Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time.

Northshore takes the privacy and security of the personal information in our care very seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,



Alan G. Nelson
General Manager

Steps You Can Take to Protect Your Personal Information

1. **Website and Enrollment.** Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports 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 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.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 160	P.O. Box 105069
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

If your username and/or password were impacted by this event, we recommend that you promptly change your password and security question or answer, as applicable, or to take other appropriate steps to protect the impacted online account and all other online accounts for which you use the same user name or email address and password or security question or answer.