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

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 2, 2021

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: Voluntary Notice of Data Event

Dear Sir or Madam:

We represent Northshore Utility District ("NUD") located at 6830 NE 185th Street, Kenmore, Washington 98028, and are writing as a courtesy to notify your office of an incident involving a third party vendor that may affect the security of personal information relating to approximately 4,900 Washington residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, NUD 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 9, 2021, NUD was informed by its check-payment processing vendor Automatic Funds Transfer Services, Inc. ("AFTS") that AFTS had experienced a ransomware attack impacting its internal servers. Initially, AFTS reported that NUD was not affected because AFTS was using its secure cloud-based service to store NUD customer data, which was not affected. Unfortunately, AFTS later indicated that a copy of the cloud-based data set may have been stored on the internal servers impacted by the ransomware incident.

AFTS's investigation is ongoing, and NUD is working with AFTS to understand the full extent and impact of the attack on NUD customer information. Although the precise number of NUD customers with personal information, if any, affected by this event has not yet been determined,

NUD is voluntarily providing notice of the event to potentially impacted customers and to your office in an abundance of caution.

The NUD customer information that could have been stored on AFTS' systems and therefore impacted by this event includes customer name, address, account balance, and financial account information.

Notice to Washington Residents

Out of an abundance of caution, NUD is providing notification to approximately 4,900 Washington residents with information about this event. NUD customers potentially affected are being mailed notice in substantially the same form as the letter attached here as ***Exhibit A***.

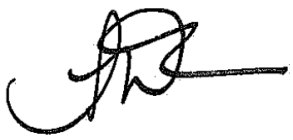
Other Steps Taken and To Be Taken

Upon discovering the event, NUD moved quickly to investigate and respond to the incident and identify potentially affected individuals. Additionally, NUD 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. NUD is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4842.

Very truly yours,



Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF:kjc

EXHIBIT A

[Date]

Customer
[Address]
[City], [State] [ZIP]

Re: Notice of Data Breach

Dear Customer:

I am writing to inform you of a security incident involving Northshore Utility District's (NUD) third-party check payment processing vendor. While the vendor's case is currently under investigation, we wanted to inform you, so you can take appropriate action necessary to protect your information from possible misuse.

Background. In an effort, to enhance data security and effectively manage workload demands with remote workers, NUD recently acquired check payment processing services through Automatic Funds Transfer Services, Inc. ("AFTS"). AFTS is a Seattle-based company with decades of experience in providing payment processing services to numerous jurisdictions and municipalities throughout Washington State and California. AFTS services provided to NUD was limited to processing payments made by check that were sent by mail.

What Happened? On February 9, 2021, the District was informed that AFTS experienced a ransomware attack on their computer systems. Initially, AFTS reported that NUD was not affected because we were using their secure cloud-based service, which was not involved. Unfortunately, AFTS later indicated that a copy of the cloud-based data set was stored on systems that were impacted by the ransomware incident. We are working with AFTS to understand the full extent and impact of the attack on NUD customer information.

What Information Was Involved? The District provides utility billing information to AFTS through a secure cloud-based portal. AFTS then receives check payments and produces an electronic image of checks for processing with NUD's bank. AFTS then produces a payment record to NUD so billing records can be updated. It is important to note, that NUD's internal systems were not affected by this attack. AFTS' investigation

is expected to confirm what, if any, NUD customer information was exposed. It is feasible that potential exposure of information includes customer names, addresses, utility account numbers, account balances and image of checks AFTS had processed.

What Are We Doing? NUD is working with cybersecurity specialists to determine the full impact of this event. We are in contact with AFTS and receiving regular updates on the status of their investigation. In the meantime, we have reestablished in-house check payment processing by our internal staff. This practice will remain in effect until further notice. As a precautionary measure, both AFTS and NUD notified law enforcement of this incident.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and credit reports for suspicious activity and promptly inform your financial institution of any anomalies. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information.*

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact us at (425) 398-4400. You may also write to NUD at: 6830 NE 185th Street, Kenmore, WA 98028.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

Alan G. Nelson
General Manager

Steps You Can Take to Help Protect Your Information

Monitor Accounts

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	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 www.equifax.com/personal/credit-report-services

Additional Information

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); and 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.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the

right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC).

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are two (2) Rhode Island residents impacted by this incident.

Washington D.C. Residents: the Office of Attorney General for the District of Columbia can be reached at: 441 4thStreet NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov.