BakerHostetler

Baker&Hostetler LLP

1170 Peachtree Street
Suite 2400
Atlanta, GA 30309-7676

T 404.459.0050
F 404.459.5734
www.bakerlaw.com

John P. Hutchins
direct dial: 404.946.9812
jhutchins@bakerlaw.com

September 3, 2020

VIA EMAIL (SECURITYBREACH@ATG.WA.GOV)

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Notice of Security Incident

Dear Attorney General Ferguson:

We are writing on behalf of our client, Osmose Utilities Services, Inc. ("Osmose"), to provide notice of a security incident involving Washington residents.[1]

Osmose recently detected unauthorized access to certain systems in its network. Osmose immediately secured the affected systems, launched an investigation to determine the nature and scope of the incident, and a specialized cybersecurity firm was engaged to assist. The investigation determined that systems containing information related to current and former employees were accessed by an unauthorized third party on July 10, 2020. The investigation could not determine precisely what information, if any, actually may have been viewed or acquired by the unauthorized person. Out of an abundance of caution, Osmose conducted a comprehensive review of the contents of the affected systems and, on August 21, 2020, learned for the first time that the systems contained the names, Social Security numbers, health insurance information and/or direct deposit information (including bank account and routing numbers) of 577 Washington residents.

On September 3, 2020, Osmose began mailing notification letters to the Washington residents in substantially the same form as the enclosed letter via U.S. First-Class mail in accordance with RCW 19.255.010. Osmose is offering eligible individuals a complimentary, one-year membership to credit monitoring and identity protection services. Osmose has also

[1] This notice does not waive Osmose's objection that Washington lacks personal jurisdiction over it regarding any claims related to this incident.

established a dedicated, toll-free call center where individuals may obtain more information regarding the incident.

To help prevent a similar incident from occurring in the future, Osmose is implementing enhanced security measures and providing additional training to employees.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

John P. Hutchins

John P. Hutchins
Partner

Osmose®

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Osmose Utilities Services, Inc. and its affiliated companies ("Osmose") value the relationship we have with our employees and former employees and understand the importance of safeguarding personal information. We are writing to inform you of an incident that involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On July 13, 2020, Osmose suffered a cyber attack against our computer systems, whereby some of our systems were encrypted. We immediately secured the affected systems, launched an investigation to determine the nature and scope of the incident, and a specialized cybersecurity firm was engaged to assist.

We restored our computer systems to fully operational. Through the forensic investigation, we identified certain systems that the unauthorized third party accessed during the incident. The accessed systems contained folders with information related to current and former employees. The investigation did not determine whether the unauthorized person actually viewed or accessed all of the files within these folders; however, we were not able to rule out that possibility. We therefore reviewed the contents of the files to identify the types of personal information involved. On August 21, 2020, we determined that one or more of these files contained your <<b2b_text_1(ImpactedData)>>.

Although we cannot confirm whether your information was viewed by an unauthorized person, we wanted to inform you of this incident and offer recommendations on ways to help protect your information. In addition, there are state laws that require us to notify you in writing of a circumstance like this. As always, we encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements for any unauthorized activity. As an added precaution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

You have until December 2, 2020 to activate your identity monitoring services.

Activation Number: <<Member ID>>

For more information on identity theft prevention and your complimentary services, please see the additional information provided in this letter.

We regret any inconvenience or concern this incident may cause. To further help protect personal information, we are taking steps to enhance our existing security protocols and re-educating our employees for awareness on these types of incidents. If you have any questions, please call 1-866-951-4186, Monday through Friday from 9:00 A.M. through 6:30 P.M Eastern Time.

Sincerely,

Ashley Moss

Ashley Moss
Vice President – Human Resources

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission,* Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If your health insurance information was involved, it is also advisable to review the billing statements you receive from your health insurer. If you see charges for services you did not receive, please contact the insurer immediately.

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze,** PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze,** PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze,** PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office,* 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us. Osmose Utilities Services, Inc. is located at 635 Hwy 74 S, Peachtree City, Georgia 30269, and can be reached at (770) 632-6700

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection | *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office,* 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov.

Rhode Island: This incident involves 68 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.