



Seyfarth Shaw LLP
233 South Wacker Drive
Suite 8000
Chicago, Illinois 60606-6448
T (312) 460-5000
F (312) 460-7000

jpriebe@seyfarth.com
T (312) 460-5608

www.seyfarth.com

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
VIA E-MAIL: idtheft@oag.state.md.us

February 23, 2024

Re: Notice of Data Incident

Dear Sir or Madam:

We represent Veolia North America, Inc., whose principal business office is located at 461 From Road, 4th Floor, Paramus, New Jersey 07652. We are writing to notify you on behalf of our clients of a data security incident involving eight (8) Maryland residents. This notice may be supplemented upon any further investigation. By providing this notice, Veolia does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the relevant state statute, or personal jurisdiction.

Background: On January 9, 2024, a ransomware incident affected some software applications and systems in a portion of Veolia North America's Municipal Water division. The Company's IT and Security Incident Response Teams were quickly mobilized, and it is actively cooperating with law enforcement and other third parties to investigate and address this incident. In response to this incident, Veolia implemented defensive measures, including taking the targeted back-end systems and servers offline until they could be restored. This incident seems to have been confined to the internal back-end systems at Veolia North America, and there is no evidence to suggest it affected the Company's water or wastewater treatment operations.

In the course of its investigation, the Company has identified a limited number of individuals whose personal information was potentially impacted. Those individuals who may have been impacted by this incident will be contacted directly by Veolia and provided additional information and assistance. Veolia is partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident and to examine additional measures the Company can take to help prevent incidents of this kind in the future.

Veolia conducted a rapid and thorough investigation, search and manual review of all the data potentially accessed or acquired by the threat actor in this event. This effort included the targeted prioritization and review of files using the Company's internal data loss prevention tool, Varonis, as well as a manual review of files using significant internal and external resources.

In addition to the short-term remediation measures described above, Veolia will (i) review and implement recommendations in the forensics report issued by CrowdStrike, and (ii) launch a campaign to reinforce cyber security, including accelerating the back-up of servers and rebuilding a new back-up solution (natively cloud) for its entire information system. Going forward, there will

be significant focus on ensuring segregation between the Company's IT networks and OT networks in order to increase protection of critical utility infrastructure and mitigate potential harm to the environment and public health and safety.

While there were several security reminders issued to employees before and during the first few weeks after the incident, a heightened awareness campaign will be launched for Veolia employees with additional cybersecurity and data protection training.

Notice to Maryland Residents: We have determined that the number of Maryland residents potentially affected by this security incident is 8. Written notice has been provided in substantially the same form the letter attached hereto as **Exhibit A**. Veolia mailed notice to impacted individuals on February 24, 2024.

Other Steps Taken and To Be Taken: Our clients are providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for 24 months through Experian at no cost to the individuals.

Additionally, Veolia's notice letters provide impacted individuals with guidance on how to better protect against identity theft and fraud. This guidance includes advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Our clients are also providing individuals with information on how to place a fraud alert and security freeze on their credit file, information on protecting against 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 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 incident, please contact us at (312) 460-5608 or jpriebe@seyfarth.com.

Very truly yours,

SEYFARTH SHAW LLP

Jason Priebe



February 24, 2024

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

K9050-L02-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L02
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



RE: Important Security Notification. Please read this entire letter.

Dear Sample A. Sample:

We are writing to let you know that Veolia North America's Municipal Water division ("our," "us," "we," or the "Company") was recently the target of a sophisticated ransomware incident, which may have involved some of your personal information. While we have no evidence of attempted or actual misuse of your information, we are providing you with information about the incident, what personal information was involved, the steps we are taking in response, and steps you may take against identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On January 9, 2024, we responded to suspicious activity involving the Company's information technology network (the "IT Network"). We immediately initiated our incident response plan to review the security of our network, engaged third-party forensic specialists to investigate the incident, and contacted law enforcement. The investigation revealed that the bad actor gained unauthorized access to Veolia's IT Network and deployed ransomware on multiple back-end systems. As a result, certain Company files were accessed and/or acquired.

You are receiving this notice because our investigation revealed evidence that personal information related to you was likely to have been impacted in the incident.

What Information Was Involved? The personal information believed to potentially be at risk includes your first and last name and one or more of the following unique identifiers: date of birth, social security number, driver's license number, or government issued identification.

What Are We Doing To Protect Your Personal Information? We took proactive steps to mitigate the impact to our Industrial Control Systems (ICS), including our Supervisory Control and Data Acquisition (SCADA) systems (collectively, "Operational Technology") by severing all connections between our IT Network and Operational Technology network. We disabled certain back-end systems in our IT Network, which caused temporary disruptions to certain systems and software (most of these back-end systems have since been restored). Moreover, we forced a reset of all passwords that grant user access to our impacted IT Network. Finally, we implemented additional security measures to fortify our IT Network's existing security measures and protocols.

What Can You Do? We encourage you to remain vigilant by regularly reviewing all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you can enroll to receive the complimentary credit monitoring service that we are offering. To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months. Outside of your access to Experian, please see the **Additional Steps to Protect Against Identity Theft and Fraud** section for information about fraud alerts and security freezes from the U.S. Federal Trade Commission and the credit reporting agencies.

If you believe there was fraudulent use of your information as a result of this incident 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 from

0000001



the date of the incident (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 Identity Restoration is available to you for 24 months 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.

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 24-month 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 April 30, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- 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 833-918-0879 by April 30, 2024. Be prepared to provide engagement number B114744 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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 file 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.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 833-918-0879 toll-free Monday through Friday from 8:00 am – 8:00 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B114744.

Sincerely,



Karine Rouge
CEO, Municipal Water
Veolia North America

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS TO PROTECT AGAINST IDENTITY THEFT AND FRAUD

Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 24-month credit monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. 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.

Equifax
P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion LLC
P.O. Box 6790
Fullerton, PA 92834-6790
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. 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 contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
<http://www.transunion.com/creditfreeze>
1-888-909-8872

In order to place the security freeze, you'll need to provide your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

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 reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Additional Helpful Resources. 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.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

*In Addition, New Mexico Consumers Have the Right to
Obtain a Security Freeze or Submit a Declaration of Removal*

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen (15) minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of pre-screening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three (3) business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen (15) minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You can contact the North Carolina Attorney General at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, Telephone: 1-877-566-7226 (Toll-free within North Carolina), 1-919-716-6000; <https://ncdoj.gov/> Identity Theft Link: <https://ncdoj.gov/protecting-consumers/protecting-your-identity/>.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request. A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities. If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report. To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above. In order to request a security freeze, you may 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. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.



