



DEV

November 10, 2025

**Re: Notice of Data Incident**

Dear [REDACTED]

Hampton Roads Sanitation District ("HRSD") writes to inform you as a current or former employee, or beneficiary of a current or former employee, of a recent data security incident that may have impacted the security of your personal information. While we are unaware of any misuse of your personal information at this time, we are providing you with details about the event, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

**What Happened?**

On October 6, 2025, we became aware of unusual activity within our network. Upon becoming aware of this activity, we immediately implemented our incident response plan and began an investigation into the nature and scope of the issue. This preliminary investigation found evidence that our network and certain files may have been accessed by an unauthorized party. In turn, we promptly engaged third-party cybersecurity specialists to provide additional assistance with our response and investigation. Based on the findings from the investigation, we diligently reviewed the potentially impacted files to identify and catalog the types of information present within them and any individuals to whom the information related. We completed our review and finalized the list of individuals to notify on November 3, 2025.

**What Information Was Involved?**

Although we have no evidence that any sensitive information has been misused by third parties as a result of this event, we are notifying you out of an abundance of caution and for purposes of full transparency. [REDACTED]

[REDACTED] may have also been impacted.

**What We Are Doing.**

We take this event seriously and the privacy, security, and confidentiality of information in our care are among our highest priorities. Upon becoming aware of the event, we moved quickly to promptly investigate and respond to the event. Specifically, we took steps to secure our systems, remediating all impacted systems, and are implementing additional technical safeguards, enhanced security measures, and updated procedures to mitigate against the risk of future issues. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so.

In light of the event, we are also providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by HaystackID specializing in fraud assistance and remediation services. While HRSD is covering the cost of these services, you will need to complete the activation process yourself.

### **What You Can Do**

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, to monitor your credit reports for suspicious or unauthorized activity, and to report any suspicious activity promptly to your bank, credit card company, or other applicable institution. Please review the enclosed *Additional Resources to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse. Furthermore, you may also activate the credit monitoring services, according to the instructions provided below, which we are making available to you at no cost.

### **Credit Monitoring Enrollment Instructions**

To enroll in the free credit monitoring services noted above, please log on to **<https://app.identitydefense.com/enrollment/activate/HRSD>** and follow the instructions provided. When prompted, please provide the following unique code to receive services: [REDACTED] In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. Enrollment requires an internet connection and e-mail address and may not be available to minors under the age of eighteen (18) years of age. Please note that, when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

### **For More Information**

If you have any questions or concerns not addressed in this letter, please call 888-844-1297 (toll free) ) during the hours of 8:00 am to 11:00 pm Eastern time, Monday through Friday and 9:00 am to 6:00 pm Saturday (excluding U.S. national holidays).

We sincerely regret any concern or inconvenience this matter may cause, and remain dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Hampton Roads Sanitation District



## **ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION**

### **Monitor Your Accounts**

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity. You may obtain a free copy of your credit report by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies. You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>.

### **Credit Freeze**

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

### **Fraud Alert**

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The agency you contact will then contact the other credit agencies.

### **Federal Trade Commission**

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General’s office in your home state and you have the right to file a police report and obtain a copy of your police report.

### **Contact Information**

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
<b>Experian</b>	P.O. Box 2002 Allen, TX 75013 1-866-200-6020 <a href="http://www.experian.com">www.experian.com</a>	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/fraud/center.html">www.experian.com/fraud/center.html</a>	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>
<b>Equifax</b>	P.O. Box 740241 Atlanta, GA 30374 1-866-349-5191 <a href="http://www.equifax.com">www.equifax.com</a>	P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 <a href="http://www.equifax.com/personal/credit-report-services/credit-fraud-alerts">www.equifax.com/personal/credit-report-services/credit-fraud-alerts</a>	P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a>
<b>TransUnion</b>	P.O. Box 1000 Chester, PA 19016 1-800-888-4213 <a href="http://www.transunion.com">www.transunion.com</a>	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 <a href="http://www.transunion.com/fraud-alerts">www.transunion.com/fraud-alerts</a>	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 <a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a>

**For Oregon residents** are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

**For Massachusetts residents** are advised of their right to obtain a police report in connection with this incident.

**For Maryland residents**, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at [www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx](http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx), or by sending an email to [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us), or calling 410-576-6491. HRSD is located at 1434 Air Rail Ave, Virginia Beach, VA 23455 and can be reached at 757-460-2261.

**For New York residents**, 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, [www.dos.ny.gov/consumerprotection](http://www.dos.ny.gov/consumerprotection); and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, [www.ag.ny.gov](http://www.ag.ny.gov).

**For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and [www.ncdoj.gov](http://www.ncdoj.gov). You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at [www.ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/](http://www.ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/).