



<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<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>> <<Last_Name>>,

<<b2b_text_2 (variable header)>>

We are writing to inform you that Lakehaven Water and Sewer District (“Lakehaven” or “we”) recently experienced a cybersecurity incident (the “Incident”) that involved your personal information (“Information”). This letter provides you with information about this Incident, our response, and information on where to direct your questions.

What Happened?

On August 25, 2025, we discovered suspicious activity on our computer systems. Upon discovery, we immediately began an investigation and took steps to contain the situation, including proactively taking systems offline, changing passwords, deploying advanced security and detection software, restoring systems from backups, and engaging leading cybersecurity professionals to assist with our investigation and response. The investigation determined that there was unauthorized access to our systems between August 22, 2025, and August 27, 2025. Thanks to our existing protections, we were able to restore our critical systems and information from existing backups. Our water and sewer services remained fully operational throughout our response.

Through our investigation, we identified that files containing your Information were obtained by an unauthorized party. Our investigation did not identify any evidence of misuse of your Information for fraud or identity theft related to the Incident.

What Information Was Involved?

Our investigation determined that the following types of Information were impacted as a result of this Incident: <<b2b_text_1 (name, data elements)>>.

What We Are Doing.

We take the security of employee Information in our care seriously. Upon identifying this Incident, we immediately implemented additional measures to further improve the security of our systems and practices. We worked with leading cybersecurity and privacy firms to aid in our investigation and response, and after determining unauthorized activity occurred on our systems, we immediately began analyzing the information involved to confirm the identities of potentially affected individuals to notify them.

What Can You Do?

While our investigation did not identify any evidence of misuse of your Information for fraud or identity theft related to the Incident, we encourage individuals to remain vigilant, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. Please also review the “Additional Resources” section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have additional questions, you may call us at (866) 613-6650 Monday through Friday from 8:00 AM to 5:30 PM Central Time, excluding some U.S. holidays.

Sincerely,

A handwritten signature in black ink, appearing to read "John Bowman", with a horizontal line extending to the right.

John Bowman

Encl.

ADDITIONAL RESOURCES

Contact information for the three (3) nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, <https://www.transunion.com/data-breach-help>, 1-833-799-5355

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one (1) or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also 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, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting Act ("FCRA").

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. 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 place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial, and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or Department of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

FTC and State Attorneys General Offices. 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 FTC and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

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

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Arizona Residents: You can obtain information from the Office of the Attorney General and the FTC about fraud alerts, security freezes, and steps you can take toward preventing identity theft. Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado Residents: You can obtain information from the Office of the Attorney General (www.coag.gov), FTC, and the credit reporting agencies about fraud alerts and security freezes. Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203, 1-720-508-6000.

For Kentucky Residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

For Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392-8222.

For North Carolina Residents: You may obtain information about preventing identity theft from the FTC (contact information above) and the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266 or 1-919-716-6400. You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, 1-877-877-9392. You are advised to report any suspected identity theft to law enforcement, the FTC, and the Oregon Attorney General.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508.

For Wyoming Residents: This notification was not delayed as a result of any law enforcement investigation.