Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

RE: Notice of Data Breach

Dear <<Full Name>>:

The City of Lubbock (the "City") is providing its customers with additional information about an issue that affected the City of Lubbock Utilities' ("COLU") payment website, which is hosted by a third-party web vendor. This website is used by COLU customers to pay City utilities bills, which may include water, wastewater, storm water and solid waste, depending on the area you live in.

We encourage customers who made or attempted to make a one-time utility bill payment on this website between December 18, 2024, and January 6, 2025, to read the below information carefully, as it contains details about this incident and steps customers can take to help protect their information.

If you did not make or attempt to make a one-time utility bill payment between December 18, 2024, and January 6, 2025, this incident did not involve your information. Additionally, customers with automatic payments set up to process their payments during this time were not affected

Please note, this incident was limited to COLU's payment website hosted by a third-party vendor, and the City's internal network was not impacted by this incident.

What Happened.

On or around January 6, 2025, the City discovered that a malicious actor had created a fake pop-up window on the COLU payment website, which requested credit card payment information from users. Customers attempting to make payments on the legitimate COLU payment website were being directed to the fake pop-up window between December 18, 2024, and January 6, 2025. Although the City has accounted for all payments made during this period and no payments were delayed, this incident may have allowed the malicious actor to collect payment card information from individuals who entered their details in the fake pop-up window during this timeframe.

What Information Was Involved.

If you made or attempted to make a one-time utility payment on the COLU payment website during this timeframe, the following information of yours may have been impacted: name, billing address, payment card number, CVV, and expiration date.

What We Are Doing.

When the City discovered the issue, it promptly disabled the COLU payment website to address the issue and engaged third-party cybersecurity specialists to investigate. By disabling the legitimate COLU payment website, customers were no longer being redirected to the fake pop-up window.

The City also performed a targeted scan of the dark web to determine whether any information involved in this incident may have been exposed. Although there have been no findings to date, the City is informing individuals about the incident and providing free credit monitoring services to those who may be involved. A description of the services being offered and instructions for how to enroll in those services are included below.

The confidentiality, privacy, and security of information entrusted to the City remains our top priority. The City has notified and is cooperating with federal law enforcement about this matter and is further enhancing our security controls to prevent a similar incident from occurring in the future.

What You Can Do.

If you made or attempted to make a payment on the COLU payment website between December 18, 2024, and January 6, 2025, we encourage you review the steps below to help protect your personal information.

1. Register for Credit and Identity Protection Services. COLU is providing individuals with access to <<CM Duration>> months of credit and identity monitoring through Equifax Credit Watch™ Gold at no cost.

Enter your Activation Code: *<<ACTIVATION CODE>>*
Enrollment Deadline: *<<Enrollment Deadline>>*

Key Features[1]

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[2] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts,[3] which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[4]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[5]

Enrollment Instructions

Go to www.equifax.com/activate
Enter your unique Activation Code of *<<ACTIVATION CODE>>* then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1] You must be over age 18 with a credit file to take advantage of this product.
[2] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.
[3] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.
[4] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

[5] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

2. Review Your Accounts for Suspicious Activity. We encourage you to remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity.

3. Order a Credit Report. If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. Contact information for the nationwide credit reporting agencies is provided in the next section.

4. Contact the Federal Trade Commission, Law Enforcement and Credit Bureaus. You may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.identitytheft.gov; call the FTC at 1-877-438-4338; or write to the FTC Consumer Response Center at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

   You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 740241 Atlanta, Georgia, 30374 www.equifax.com 1-800-525-6285	P.O. Box 9701 Allen, TX 75013 www.experian.com 1-888-397-3742	P.O. Box 2000 Chester, PA 19022 www.transunion.com 1-800-916-8800

5. Additional Rights Under the FCRA. 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by: (i) visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf; or (ii) by writing to Consumer Financial Protection Bureau, 1700 G Street, NW, Washington, DC 20552.

6. Request Fraud Alerts and Security Freezes. You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

   In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze at no cost to you:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ 1-888-298-0045	P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze 1-888-397-3742	P.O. Box 160 Woodlyn, PA 19094 http://www.transunion.com/creditfreeze 1-888-916-8800

Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

- Your full name, with middle initial as well as Jr., Sr., II, etc.
- Social Security number
- Date of birth
- Current address and all addresses for the past two years
- Proof of current address, such as a current utility bill or telephone bill
- Legible copy of a government-issued identification card, such as a state driver's license, state identification card, or military identification.

After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

For More Information.

We understand that you may have additional questions that have not been addressed. We have established a dedicated toll-free call center to respond to additional inquiries about this matter. You can contact the call center at [redacted], Monday through Friday, between 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays. Alternatively, you can contact the City by writing to us at 1314 Avenue K, Lubbock, TX 79401 or calling 1-806-775-3000. We apologize for any inconvenience this may have caused and remain committed to the security of our customers' information.

Sincerely,

City of Lubbock Utilities