



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
 <<address\_1>>  
 <<address\_2>>  
 <<city>>, <<state\_province>> <<postal\_code>>  
 <<country >>

Esta carta contiene información importante sobre su cuenta de agua de la ciudad de Aurora. Por favor de llamar a 1-844-931-1876 para más información.

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

The Aurora Water Department (“Aurora Water”) — which serves the City of Aurora, Colorado (“City”) — recently became aware of an information security incident. The incident may affect only the personal information of certain Aurora Water customers who submitted payment information through Aurora Water’s Click2Gov payment system between approximately August 30, 2019, and October 14, 2019. We are providing this notice to inform you of the incident and to call your attention to some steps you can take to help safeguard yourself. We sincerely regret any concern this may cause you.

### What Happened

The incident only involves the Aurora Water Click2Gov customer payment software, which is issued and maintained by CentralSquare Technologies (“CentralSquare”), a third party that provides payment processing services. Upon learning of a potential issue, we launched an investigation with the assistance of a leading cybersecurity forensics firm. Through the investigation, we learned that an unauthorized actor — not associated with Aurora Water or the City — modified a piece of computer code that the Click2Gov software uses. This modified computer code could have run on the internet browser of visitors to Aurora Water’s payment website and may have captured limited personal information such as payment card information entered for one-time payments or to set up new reoccurring payments. This incident did not affect Aurora Water customers already set up to use the Click2Gov automatic payment functionality or those that submitted payments in alternative manners. The modified code was likely active between approximately August 30, 2019 and October 14, 2019. **Please note, the Click2Gov software is not used by, and does not affect, any other City departments.**

### What Information Was Involved

Aurora Water customers who entered payment information through its website using the Click2Gov online bill payment system between approximately August 30, 2019 and October 14, 2019 could be affected. Aurora Water has received information from CentralSquare regarding the incident and based on this, and our own investigation, we believe that the incident may have affected limited personal information, such as first name, last name, billing address, payment card type, payment card number, payment card verification value and payment card expiration date. Please note that other personal information such as Social Security number or government-issued identification numbers were not affected by this incident.

### What We Are Doing

We deeply regret that this incident with our third-party vendor occurred. As stated previously, we took prompt action in response to the incident. We launched an internal investigation and retained a leading cybersecurity forensic firm to assist in our investigative process. We took the Click2Gov customer payment site down. We are continuing to review and enhance security measures to help prevent something like this from happening again in the future. In addition, we have been working with and continue to cooperate with law enforcement. To support our customers, we have also set up a dedicated page on our website — AuroraGov.org/C2GAdvisory — where we will post information about this incident.

As you are aware, Aurora Water began notifying customers last spring that it would transition fully to a different online bill payment processing system, called Paymentus, which Aurora Water formally launched in November of this year. This incident is not related to our transition. The Paymentus system was not affected by this incident and can be accessed for online payments by visiting AuroraWater.org. Please note, the incident did not affect Aurora Water's other payment systems such as pay-by-phone, payments made by mail or in person, or through other third-party services such as bank bill payment options.

To help monitor your identity, we have secured the services of Kroll, a global leader in risk mitigation and response, to provide identity monitoring at no cost to you for one year. Kroll's team has extensive experience helping people who may have sustained an unintentional exposure of personal information. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

### **What You Can Do**

As outlined above, we are offering identify monitoring services at no cost to you for one year. To activate your membership and start monitoring your personal information please follow the steps below:

- Visit [enroll.idheadquarters.com](http://enroll.idheadquarters.com) to activate and take advantage of your identity monitoring services.
- You have until **March 29, 2020** to activate your identity monitoring services.
- Membership Number: <<Member ID>>

For more information about these services, please refer to the "Additional Information" reference guide attached to this letter.

You can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of the report. You may need to give copies of the police report to creditors to clear up your records. You can also review your financial account statements to determine if there are any discrepancies or unusual activity listed. If you see anything you do not understand, call the financial institution immediately.

You may choose to notify your bank to see if there are any additional protections available to help to prevent someone from accessing your accounts or initiating transactions without your permission. As a general practice, you can regularly monitor your accounts for unusual activity or any transactions you do not recognize. If you find anything unusual, contact your financial institution immediately.

You may also carefully review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and continue to monitor statements for any unusual activity going forward. If you see anything you do not recognize, you should immediately notify the issuer of the credit or debit card as well as the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

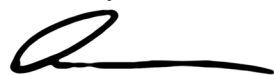
### **Other Important Information**

We have included the "Additional Information" reference guide, below, that describes additional steps that you may take to help better safeguard yourself, including recommendations by the FTC regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

### **For More Information**

For more information about this incident, you may call 1-844-931-1876 between the hours 7:00 a.m. to 4:30 p.m. Mountain Time, Monday through Friday excluding holidays, or visit our website at [AuroraGov.org/C2GAdvisory](http://AuroraGov.org/C2GAdvisory).

Sincerely,



Greg Baker  
Manager of Public Relations | City of Aurora | Aurora Water

## ADDITIONAL INFORMATION

**Additional Details Regarding Your Kroll Identity Monitoring Services:** You've been provided with access to the following services<sup>1</sup> from Kroll.

- **Single Bureau Credit Monitoring:** You will receive alerts when there are changes to your credit data — for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's 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 access 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 co do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

**Review Accounts and Credit Reports:** You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an 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 by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

**For residents of Maryland:** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us).

**For residents of New York:** You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/internet/privacy-and-identity-theft>.

**For residents of North Carolina:** You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, [www.ncdoj.gov](http://www.ncdoj.gov).

### **Security Freezes and Fraud Alerts:**

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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

<sup>1</sup> 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.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this guide.

**Additional Information for New Mexico Residents:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Here is a summary of your major rights under the FCRA:

- You have the right to be told if information in your file has been used against you;
- You have the right to receive a copy of your credit report and the right to ask for a credit score;
- You have the right to dispute incomplete or inaccurate information;
- You have the right to dispute inaccurate, incomplete, or unverifiable information;
- You have the right to have outdated negative information removed from your credit file;
- You have the right to limit access to your credit file;
- You have the right to limit "prescreened" offers of credit and insurance you get based on information in your credit report;
- You have the right to seek damages from violators; and
- You have the right to place a "security freeze" on your credit report.

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. 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 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 remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and may need to provide 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;
- (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; and
- (4) payment of a fee, if applicable.

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 business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen 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 prescreening 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 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 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.

For more information, including information about additional rights, you can visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>, <https://www.consumerfinance.gov/learnmore/>, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

### **National Credit Reporting Agencies' Contact Information**

#### **Equifax**

([www.equifax.com](http://www.equifax.com))

#### **General Contact:**

P.O. Box 740241

Atlanta, GA 30374

800-685-1111

#### **Fraud Alerts and Security Freezes:**

P.O. Box 740256, Atlanta, GA 30374

#### **Experian**

([www.experian.com](http://www.experian.com))

#### **General Contact:**

P.O. Box 2002, Allen, TX 75013

888-397-3742

#### **Fraud Alerts and Security Freezes:**

P.O. Box 9556, Allen, TX 75013

#### **TransUnion**

([www.transunion.com](http://www.transunion.com))

#### **General Contact, Fraud Alerts and**

#### **Security Freezes:**

P.O. Box 2000

Chester, PA 19022

888-909-8872

National Credit Reporting Agencies'  
Contact Information