Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

This letter follows my June 6, 2019 email in which I notified you about a data security incident the City of Longmont recently experienced. We write to provide you with additional information about the incident and our response. We also wanted to provide you with information about steps you can take to protect your information and, as referenced in my earlier email, offer you complimentary credit monitoring services for 12 months.

What Happened? On June 6, 2019, an email with the subject line "Munis 2018 Financial Close" was inadvertently sent to unintended recipients. The email included an attachment that contained the personal information of city employees. Upon discovering the incident, we immediately worked with our information technology partners to recall the message, delete all copies of the message and attachment from all email accounts, and determine whether the message was forwarded to any email accounts outside our system. We also notified all city employees of the incident and directed them to ensure that the file was deleted, and not printed, saved, or imaged in any manner. We are now providing you with additional information about the incident and steps you can take to protect your personal information. We are also offering you 12 months of complimentary credit monitoring services.

What Information Was Involved? The information may have your involved name, address, and Social Security number.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We are now providing you with information about steps you can take to help protect your personal information and are offering you 12 months of complimentary credit monitoring services.

What You Can Do: At this time, we have no indication of any misuse of the information that was erroneously emailed. However, as a precaution, we are providing you with additional information about how to protect your personal information on the pages following this letter. In addition, you can enroll in the three-bureau credit monitoring service that we are offering for 12 months at no cost to you. The services are known as *my*TrueIdentity and are being provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies. The service will notify you if there are critical changes to your credit files at TransUnion,® Experian,® and Equifax,® including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.) You may enroll in the services online or via U.S. mail delivery by following the instructions below.

- To enroll in this service via the Internet, go to the myTrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<Six-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the credit monitoring service anytime between now and <<Enrollment Deadline>>. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

For More Information: If you have questions, please call 877-641-8869, Monday through Friday, 7:00 a.m. to 7:00 p.m. Mountain Time. To enroll in the credit monitoring services that we are offering for 12 months at no cost, or to speak with a TransUnion representative if you believe you may be the victim of identity theft, please call TransUnion's Fraud Response Services toll-free hotline at 1-855-288-5422.

We take the privacy and security of all information within our control very seriously. We apologize for any worry or inconvenience that this incident may cause.

Sincerely,

Harold Dominguez
City Manager
City of Longmont, Colorado

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There should be no charge with placing a security freeze on your credit file. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.