BAKERSFIELD
THE SOUND OF *Something Better*

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

<<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Notice of Data Breach

Dear <<<LastName>>,

The City of Bakersfield ("Bakersfield") values the relationship we have with our customers and understands the importance of protecting their information. We are writing to inform you of an incident that may have involved some of that information. Bakersfield takes issues of Internet security and data confidentiality very seriously. This letter describes what happened, measures we have taken, and some steps you can take in response.

What Happened

After receiving reports that fraudulent activity was detected on payment cards used legitimately on our website, Bakersfield immediately launched an investigation. Through our investigation, we determined that an unauthorized party had inserted unauthorized code into Bakersfield's online payment system, Click2Gov, which is developed by a third-party vendor, CentralSquare Technologies ("CentralSquare"). The unauthorized code was designed to capture payment card data and other information entered on Bakersfield's Click2Gov online payment system between the dates of July 30, 2019 and September 5, 2019. Upon learning of the unauthorized code, Bakersfield began working with CentralSquare to remove the unauthorized code from our website's Click2Gov online payment system. Bakersfield has also updated its computer systems to protect against future insertion of the unauthorized code. We are notifying you because you made a payment on Bakersfield's Click2Gov online payment system during this time period.

What Information was Involved

The information entered on the Click2Gov online payment system on Bakersfield's website includes name, address, email address, payment card number, expiration date, and card security code (CVV).

What We are Doing

Upon learning of the incident, Bakersfield worked swiftly to address the issue by immediately removing the malicious code from the Click2Gov online payment system on our website and initiating an expanded security review with CentralSquare and a leading data forensics firm specializing in cybersecurity incidents. To prevent another incident, we are enhancing our existing security protocols and implementing additional security measures. Bakersfield also contacted law enforcement and is continuing to support law enforcement's investigation. As a result of this incident, Bakersfield is ending its relationship with Click2Gov, and is currently working to transition to a new vendor for city payment processing.

What You Can Do

We remind you to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized charges. You should immediately report any unauthorized charges to your card issuer because payment card network rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the pages that follow this notice for additional steps you may take.

For More Information

We regret any inconvenience or concern this incident may have caused you. If you have any questions, please call 1-877-514-0869, Monday through Friday, between 8:00 a.m. to 5:00 p.m., Pacific Time.

Sincerely,

Randy McKeegan

Randy McKeegan
Finance Director

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

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

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 Federal Trade Commission and/or the California Attorney General's office. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.ftc.gov/idtheft, 1-877-IDTHEFT (438-4338)

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one (1) year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below: ·

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com

TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.