BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Patrick H. Haggerty
direct dial: 513.929.3412
phaggerty@bakerlaw.com

July 16, 2018

VIA OVERNIGHT MAIL

Gordon MacDonald
Office of the Attorney General
33 Capitol St.
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

I am writing on behalf of my client, the City of Bozeman, Montana ("Bozeman" or the "City"), to notify you of a security incident involving New Hampshire residents.[1]

On or around October 29, 2017, after Bozeman received reports that certain customers had experienced fraud on payment cards after they were legitimately used on Bozeman's online utility payment system, Superion's Click2Gov, Bozeman immediately began an investigation, took the server offline and rebuilt it, and engaged a computer forensic firm to assist. After conducting a detailed and lengthy forensic investigation, neither Bozeman nor the computer security firm retained by Bozeman was able to uncover any evidence that payment card information was at risk. Subsequently, a different forensic firm engaged by Superion, the vendor that developed and maintains the Click2Gov software, informed the City that it had discovered evidence affecting other communities throughout the country that an unauthorized individual had gained access to payment card information through the Click2Gov system and may have been able to do the same with the City.

On July 3, 2018, Superion notified the City that payment card information entered into the City's Click2Gov system from July 1, 2017 through October 24, 2017 may have been captured. The information that could have been captured includes cardholder names, addresses, payment card numbers, expiration dates and card verification codes (CVV).

[1] This report is not, and does not constitute, a waiver of personal jurisdiction.

In accordance with N.H. RSA § 359-C:20(IV), on Friday, July 20, 2018, Bozeman will mail notification letters to three New Hampshire residents that may have been affected by this incident. A copy of the notification letter is attached. Bozeman is not able to identify all of its customers that submitted payment card information during the at-risk window; therefore, Bozeman, in accordance with N.H. RSA § 359-C:20(III)(d), is providing substitute notice by posting a statement about the incident to its website and issuing a press release. Bozeman is also providing a dedicated call center that customers can contact with any questions they may have.

To prevent this type of incident from happening again the City put into place security upgrades in consultation with its forensic investigator and continues to work with Superion to take steps to strengthen the security of the Click2Gov utility payment site.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Patrick H. Haggerty
Partner

Enclosure

Company Logo

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

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

Dear <<Name 1>>:

Securing and protecting our customer's confidential information is a top priority for the City of Bozeman and it is a responsibility we take very seriously. Regrettably, we are writing to notify you of an incident that involved your payment card information. This notice describes what happened, the actions the City has taken in response, and some steps that you can take to help protect your information.

What Happened

In the late fall of 2017, after the City received reports that certain utility customers had experienced fraud on payment cards after they were legitimately used on the City's online utility payment system, Superion's Click2Gov, the City immediately began an investigation, took the server offline and rebuilt it, and engaged a computer forensic firm to assist. After conducting a detailed and lengthy investigation, neither the City nor the computer forensic firm retained by the City was able to uncover any evidence that payment card information was at risk. Subsequently, a different forensic firm engaged by Superion, the vendor that developed and maintains the Click2Gov software, informed the City that it had discovered evidence affecting other communities throughout the country that an unauthorized individual had gained access to payment card information through the Click2Gov system and may have been able to do the same with the City.

On July 3, 2018, Superion notified the City that payment card information entered into the City's Click2Gov system from July 1, 2017 through October 24, 2017 may have been captured. The information that could have been captured includes cardholder names, addresses, payment card numbers, expiration dates and security codes.

The period for which payment card information was potentially captured is only between July 1, 2017 and October 24, 2017. Only the following City utility customer's payment card information is at risk: customers going online into the Click2Gov system and making a one-time payment with a payment card, customers going into the Click2Gov system and manually selecting a payment card saved in the Click2Gov system's "wallet" for a one-time payment, and customers who made one-time payments with a payment card by calling the City and speaking with a staff person.

Utility customers who are NOT affected by this incident include: (i) utility customers who came into the City and paid in person using cash, a personal or business check, or swiped a payment card at the City's finance desk; (ii) utility customers who mailed in personal or business checks; (iii) utility customers who

called into the City's automated phone system and paid with a payment card; (iv) utility customers who set up automatic payments from a payment card using the City's Click2Gov system; and (v) utility customers who set up bill pay from a customer's personal or business bank account where the payment was made by mailed or electronic check.

In addition, no evidence has been found that indicates any other online payment service provided by the City using Superion's Click2Gov has been impacted including payments made using Superion's Click2Gov for building permits, business license renewals, and payments for special assessments.

What Information Was Involved

Information entered into the City's online utility payment system Click2Gov between July 1 and October 24, 2017 may have been captured by an unauthorized individual. This information included your name, address, payment card number ending in [XXXX], expiration date, and card verification code (CVV).

What we are Doing

Caring for our residents is a top priority for the City and we have worked swiftly to address this issue. To prevent this type of incident from happening again we put into place security upgrades in consultation with our forensic investigator and continue to work with Superion to take steps to strengthen the security of the Click2Gov utility payment site.

What You Can Do

We encourage you to remain vigilant to the possibility of fraud by reviewing your financial statements for any unauthorized activity. You should immediately report any unauthorized charges to your financial institution because the major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported. The phone number to call is usually on the back of your payment card. You should also review the additional information on the following page on ways to protect yourself.

For More Information

We regret any inconvenience or concern that may result from this incident. Additional information can be found on the City's website at www.bozeman.net/security. If you have any questions, please call 1-888-236-0444 between 7:00 AM through 7:00 PM Mountain Time, Monday through Friday.

Sincerely,

Signature Image

Andrea Surratt
City Manager

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We remind you to remain 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:

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

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 Attorney General's office in your state. 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, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you are a resident of Connecticut, Maryland, Montana or North Carolina, you may contact and obtain information from your state attorney general at:

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us,
1-888-743-0023 (toll free when calling within Maryland)
(410) 576-6300 (for calls originating outside Maryland)

Montana Attorney General's Office, P.O. Box 200151, Helena, MT 59620-0151, 1-800-481-6896, https://dojmt.gov/consumer/

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400

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 at least 90 days. 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 may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from

accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three (3) major reporting agencies by regular, certified, or overnight mail 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 (5) 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 three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) 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, you must call or send a written request to the credit reporting agencies by mail 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 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail 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 three (3) business days after receiving your request to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA

(https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.