

BakerHostetler

RECEIVED

FEB 12 2020

CONSUMER PROTECTION

Baker & Hostetler LLP

Washington Square, Suite 1100  
1050 Connecticut Avenue, N.W.  
Washington, DC 20036-5403

T 202.861.1500  
F 202.861.1783  
www.bakerlaw.com

Eulonda G. Skyles  
direct dial: 202.861.1555  
eskyles@bakerlaw.com

February 11, 2020

**VIA OVERNIGHT MAIL**

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

*Re: Security Incident Notification*

Dear Attorney General MacDonald:

We are writing on behalf of our client, The City of Fremont, Nebraska ("Fremont"), to notify your office of a security incident involving one New Hampshire resident.

On October 18, 2019, Fremont received customer reports that fraudulent activity was occurring on Click2Gov, a third party-operated website which allows our utility customers to use debit and credit cards to pay their utility bills. In response, Fremont immediately launched an investigation and contacted the Click2Gov vendor CentralSquare Technologies ("CentralSquare"). Out of an abundance of caution, and to reduce potential exposure for our customers, Fremont temporarily suspended access to its Click2Gov website on October 25, 2019 while investigating the matter. On November 6, 2019, we received confirmation from CentralSquare that an unauthorized party had inserted unauthorized code on Fremont's Click2Gov website which was designed to capture name, address, payment card number, security code, expiration date, and email address entered by customers on the Click2Gov online payment system between the dates of August 31, 2019 and October 14, 2019. Upon learning this information, Fremont began working with CentralSquare to remove the unauthorized code and took measures to protect against future insertion of the unauthorized code.

Fremont has also cooperated with local and federal law enforcement concerning this incident. Following further investigation and analysis, we are now notifying the one New Hampshire resident about this event and on February 10, 2020, Fremont mailed written notification to the potentially affected New Hampshire resident in accordance with N.H. Rev. Stat. Ann. § 359-C:20

February 11, 2020

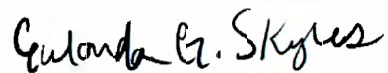
Page 2

in substantially the same form as the enclosed letter<sup>1</sup>. Fremont also provided a telephone number for potentially affected individuals to call with any questions they may have.

To help prevent a similar incident from occurring in the future, we are enhancing existing security measures on our Click2Gov site.

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

Sincerely,

A handwritten signature in black ink that reads "Eulonda G. Skyles". The signature is written in a cursive, flowing style.

Eulonda G. Skyles  
Partner

Attachments

---

<sup>1</sup> This report does not waive Fremont's objection that New Hampshire lacks personal jurisdiction over this matter. Further, Fremont reserves all rights to assert sovereign immunity in any action or legal proceeding related to this matter.



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

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

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

The City of Fremont, Nebraska ("Fremont") values its relationships with our customers and understands the importance of protecting their information. Fremont takes issues of Internet security and data confidentiality very seriously. Regrettably, we are writing to inform you of an incident involving some of your information. This notice explains the incident, measures we have taken, and steps you can take in response.

On October 18, 2019, Fremont received customer reports that fraudulent activity was occurring on Click2Gov, a third party-operated website which allows our utility customers to use debit and credit cards to pay their utility bills. In response, Fremont immediately launched an investigation and contacted the Click2Gov vendor CentralSquare Technologies ("CentralSquare"). Out of an abundance of caution, and to reduce potential exposure for our customers, Fremont temporarily suspended access to its Click2Gov website on October 25, 2019 while investigating the matter. On November 6, 2019, we received confirmation from CentralSquare that an unauthorized party had inserted unauthorized code on Fremont's Click2Gov website which was designed to capture name, address, payment card number, security code, expiration date, and email address entered by customers on the Click2Gov online payment system between the dates of August 31, 2019 and October 14, 2019. Upon learning this information, Fremont began working with CentralSquare to remove the unauthorized code and took measures to protect against future insertion of the unauthorized code. Fremont has also cooperated with local and federal law enforcement concerning this incident. Following further investigation and analysis, we are now notifying you about this event because our records show that you made a payment on Fremont's Click2Gov online payment system during the time period when the fraudulent activity occurred.

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.

We regret any inconvenience or concern this incident may have caused you. To help prevent a similar incident from occurring in the future, we are enhancing existing security measures on our Click2Gov site. If you have any questions, please call [1-781-326-7777](tel:1-781-326-7777), Monday through Friday, from 8:00 a.m. to 5:00 p.m., Central Time.

Sincerely,

A handwritten signature in black ink that reads "Brian Newton".

Brian Newton  
City Administrator  
City of Fremont  
400 E. Military Ave.  
Fremont, NE 68025

## 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](http://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](http://www.experian.com), 1-888-397-3742

*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://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](http://www.ftc.gov/idtheft)

**If you are a resident of Maryland or New York**, you may contact and obtain information from your state attorney general or state regulator at:

*Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023 / (410) 576-6300 (for calls originating outside Maryland), [www.oag.state.md.us](http://www.oag.state.md.us)

*New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>

*New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

**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 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 (7) 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](http://www.experian.com)
- TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://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 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 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](http://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.