

RECEIVED

JAN 14 2020

CONSUMER PROTECTION



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

January 10, 2020

INTENDED FOR ADDRESSEE(S) ONLY

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent the City of Port Orange (“the City”) located at 1000 City Circle, Port Orange, FL 32129, and are writing to notify your office of an incident that may affect the security of some personal information relating to three (3) New Hampshire residents that may have been affected by the CentralSquare Technologies (“CentralSquare”) data security incident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this voluntary notice, the City does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, personal jurisdiction, or sovereign immunity.

Nature of the Data Event

On November 6, 2019, the City received notice from CentralSquare of a potential data security issue within the online payment portal, Click2Gov, which is managed and operated by that vendor. The notice indicated that alterations to Click2Gov’s applicable code could have enabled the unauthorized access to certain payment card information from the customer’s internet browser window during a payment transaction. On December 4, 2019, CentralSquare confirmed that the time period in which the payment transactions may have been affected is from August 27, 2019 through October 26, 2019.

CentralSquare advised that the unauthorized code was capable of capturing customer information, such as name, address, credit/ debit card number, card type, printed security code, and expiration date.

Notice to New Hampshire Residents

CentralSquare is assisting affected entities with notifying potentially impacted individuals. On January 10, 2020, the City, through CentralSquare, provided written notice of this incident to affected individuals, which includes three (3) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

We take the confidentiality, privacy, and security of personal information very seriously. The City has strict security measures in place to protect information in our care. After receiving notice from CentralSquare, the City took steps to understand the impact the CentralSquare data security incident had on City data. Third-party forensic investigators were engaged, and with their assistance, the investigation determined that payment card information entered from August 27, 2019 through October 18, 2019 could have been affected by the CentralSquare incident. Upon confirmation of this information, the City worked to identify those individuals who may have made payments during this period. The City also discontinued use of the Click2Gov website while it assessed the security of the site. Additionally, the City took steps to confirm and further strengthen the security of its systems and the City is reviewing its security policies and procedures as part of its ongoing commitment to information security.

The City is working with law enforcement and notified relevant regulators. CentralSquare is offering the City's customers a twelve-month subscription to a free credit monitoring service offered through TransUnion.

Additionally, the City is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. The City is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Office of the New Hampshire Attorney General

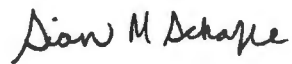
January 10, 2020

Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,



Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/jc1

EXHIBIT A



CITY OF PORT ORANGE

1000 CITY CENTER CIRCLE
PORT ORANGE, FLORIDA 32129
TELEPHONE 386-506-5500
www.Port-Orange.org

[First Name] [Last Name]

[Address]

[City, State, Zip]

[Date]

RE: Notice of Data Breach

Dear [Name],

The City of Port Orange (“the City”) is writing to notify you because you may have been affected by the CentralSquare Technologies (“CentralSquare”) data security incident. CentralSquare is a third-party vendor that provides utility billing services to the City. To date, CentralSquare has not reported that your personal information has been misused as a result of this incident. Nevertheless, we are notifying you so you are aware of the incident and may take steps to better protect your personal information should you feel it is appropriate to do so.

What Happened? On November 6, 2019, the City received notice from CentralSquare of a potential data security issue within the online payment portal, Click2Gov, which is managed and operated by that vendor. The notice indicated that alterations to Click2Gov’s applicable code could have enabled the unauthorized access to certain payment card information from the customer’s internet browser window during a payment transaction. On December 4, 2019, CentralSquare confirmed that the time period in which the payment transactions may have been affected is from August 27, 2019 through October 26, 2019.

What Information Was Involved? CentralSquare advised that the unauthorized code was capable of capturing customer information, such as name, address, credit/ debit card number, card type, printed security code, and expiration date. Our records indicate that you made a one-time payment or set up recurring payments during this time period. Therefore, it is possible that your information could have been obtained by an authorized party.

What We Are Doing. We take the confidentiality, privacy, and security of personal information very seriously. The City has strict security measures in place to protect information in our care. After receiving notice from CentralSquare, we took steps to understand the impact the CentralSquare data security incident had on City data. Third-party forensic investigators were engaged, and with their assistance, the investigation determined that payment card information entered from August 27, 2019 through October 18, 2019 could have been affected by the CentralSquare incident. Upon confirmation of this information, the City worked to identify those individuals who may have made payments during this period. The City also discontinued use of the Click2Gov website while it assessed the security of the site. Additionally, the City took steps to confirm and further strengthen the security of its systems and the City is reviewing its security

policies and procedures as part of its ongoing commitment to information security. The City is working with law enforcement and notified relevant regulators.

While CentralSquare has not reported misuse of your specific information, as an added precaution, they are offering you a twelve-month subscription to a free credit monitoring service offered through TransUnion. For instructions on how to enroll, please refer to the attached brochure.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You may review the information contained in the enclosed “Steps You Can Take to Protect Your Information” for more information on how to better protect your personal information. You may also enroll to receive the identity and credit monitoring services that are being made available to you.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, you may contact 855-930-0684, which can be reached Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. You may also contact to us directly at 386-506-5720 or write to us directly at ATTN: Customer Service, City of Port Orange, 1000 City center Circle, Port Orange, FL 32129 or customerservice@port-orange.org.

We take very seriously the security of the personal information that our customers entrust into our care and regret any inconvenience caused by this incident. Working to ensure that this does not happen again is one of our highest priorities.

Sincerely,



Dr. Scott R. Neils
CFO and Finance Director
City of Port Orange

Enroll in Credit Monitoring:

[INSERT CREDIT MONIOTRING INFORMATION HERE]

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and to detect error over the next 12 to 24 months. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

| | | |
|--|--|--|
| Experian PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html | TransUnion P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com/credit-freeze | Equifax PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services |
|--|--|--|

In order 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

| | | |
|--|--|---|
| Experian P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html | TransUnion P.O. Box 2000 Chester, PA 19106 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert | Equifax P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services |
|--|--|---|

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.