Click2Gov Customer Questions and Answers

(Q) **What Happened?**

(A) Our payment services vendor, CentralSquare Technologies ("CentralSquare"), recently notified us of a security incident involving the CentralSquare online payment service Click2Gov. CentralSquare reported that this incident could have resulted in unauthorized access to personal information. As such, the City immediately commenced an investigation to determine the nature and scope of this incident and its impact on City data.

(Q) **Who is CentralSquare Technologies and why did they have my information?**

(A) CentralSquare is a third-party vendor that provides services to the City including utility bill payment services.

(Q) **How was the issue discovered?**

(A) CentralSquare contacted the City regarding an incident that may have affected data relating to customer.

(Q) **Does this affect my banking auto-draft payment to Dothan Utilities?**

(A) No. There is no effect to banking auto-draft customers.

(Q) **Does this affect my payments to Dothan Utilities I pay through my bank, such as bill pay options?**

(A) *No. There is no effect when paying from your bank.*

(Q) **Is it safe to make online payments?**

(A) *We take the security of the personal information in our care very seriously. CentralSquare reported that the incident has been contained. The City has implemented additional precautionary measures to minimize potential attacks on the Click2Gov system.*

(Q) **What kind of measures have been taken to make sure this doesn't happen again?**

(A) *The City has implemented all recommendations from CentralSquare, which include, a new computer server, a new installation of the Click2Gov application by CentralSquare technicians, and a file-level security monitoring system added to the new server.*

(Q) **Does the City of Dothan plan to engage outside experts to assist in investigations into the potential data privacy issue?**

(A) *Yes. The City Commissioners voted to engage a leading forensic investigation firm to assist with our investigation and response to the CentralSquare event.*

The City Commissioners also voted to engage the Mullen Coughlin LLC ("Mullen Coughlin") to assist the City of Dothan and its attorneys with issues relating to this situation.

(Q) **What are the next steps for the City of Dothan?**

(A) *With the assistance of the third-party forensic investigation firm, we are conducting a forensic analysis of the data to determine the nature and scope of the potential data security event.*

(Q) **When will I and how will I be notified if I was one of the accounts compromised?**

(A) Our investigation is ongoing, if after the investigation has concluded, it is determined that the data privacy issue affected cardholder information, affected cardholders will be notified by mail as soon as the determination is made.

(Q) **Will the City provide credit protection or credit monitoring services if I have been affected?**

(A) The City is working with relevant parties, including CentralSquare, to determine the best way to assist potentially affected individuals.

(Q) **What can I do to protect against identity theft or fraud?**

(A) Steps an individual can take to protect against identity theft and fraud include:

- *Monitoring your financial statements carefully. If you see any unauthorized or suspicious activity, promptly contact your bank, credit union, or credit card company.*
- *Monitoring your credit reports for suspicious or unauthorized activity. 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.*
- *Placing a fraud alert on your credit file. 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. Contact the three major credit bureaus directly to place a fraud alert on your credit file.

- *Placing a security freeze on your credit file. A security freeze 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. Contact the three major credit bureaus directly to place a security freeze on your credit file.*
- *Contacting the Federal Trade Commission and your state Attorney General to learn more about identity theft, fraud alerts, security freezes, and other steps you can take to protect yourself. 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.*
- *Reporting incidents of suspected or actual identity theft or fraud to law enforcement, the Federal Trade Commission, and your state Attorney General.*

(Q) **What is the purpose of a "fraud alert"?**

(A) A fraud alert tells creditors to take reasonable steps to verify identity before they open a new credit account under your Social Security number.

(Q) **What is the purpose of a security freeze?**

(A) A security freeze is designed to prevent a credit reporting company from releasing your credit report without your consent.

(Q) **Should I check my credit report?**

(A) You should monitor your credit report regardless of whether your information has been exposed or you think you may be a victim of identity theft or fraud. Every U.S. consumer over the age of eighteen can receive one free credit report every twelve months by contacting one of the three national credit bureaus or through the Annual Credit Report Service by visiting www.annualcreditreport.com or calling toll-free, 1-877-322-8228.

(Q) **I think I may be a victim of identity theft. What should I do?**

(A) If you believe you are a victim of attempted or actual identity theft or fraud, we encourage you to take the following steps:

- *Contact your financial institution to protect or close any accounts that have been tampered with or opened fraudulently.*
- *Enroll in the Credit Monitoring and Identity Restoration services provided by Transunion.*
- *Contact the credit reporting agencies to place a "fraud alert" or a "credit freeze" on your credit reports.*
- *File a police report with your local police department and ask for a copy for your records.*
- *File a complaint with the Federal Trade Commission at: https://www.identitytheft.gov/.*
- *File a complaint with your state attorney general.*
- *Keep good records.*
    - *Keep notes of anyone you talk to regarding this incident, what s/he told you, and the date of the conversation;*
    - *Keep originals of all correspondence or forms relating to the suspicious activity, identity theft, or fraud; and*
    - *Retain originals of supporting documentation, such as police reports and letters to and from creditors; send copies only.*
- *Keep old files, even if you believe the problem is resolved.*