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

1275 Drummers Lane, Suite 302
Wayne, PA 19087

October 28, 2020

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notification
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Technology Management Resources, Inc. Data Event

Dear Sir or Madam:

We represent the City of Bettendorf, Iowa (the "City") located at 1609 State Street, Bettendorf, Iowa 52722, and are writing to notify your office of an incident that may affect the security of some personal information relating to five thousand three hundred eighty-seven (5387) Iowa residents that may have been affected by the Technology Management Resources, Inc. ("TMR") data security incident.

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the City does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, personal jurisdiction, or sovereign immunity.

Nature of the Data Event

TBK Bank ("TBK"), the City's third-party treasury management services vendor, which includes utility payment processing, has an agreement with TMR to provide Lockbox Payment Processing services for TBK on behalf of the City. On August 27, 2020, the City received notice from TBK of the TMR data security incident. The notice from TBK indicated that an unauthorized actor had gained access to TMR's systems and, consequently, may have been able to access images of checks

that were sent to TBK's Lockbox. TBK also provided a list of individuals associated with the City that TMR believed may have been affected by the incident.

Upon receipt of the notice, the City immediately commenced an investigation to determine the nature and scope of the underlying event. On September 17, 2020, TBK confirmed that the unauthorized actor had access to the TMR systems from June 1, 2020 to July 1, 2020. Upon using the updated information, the City was able to complete its investigation and confirmed personal information as defined by Iowa Code § 715C.1 could have been subject to unauthorized access or acquisition including name, financial account number, and routing number. To date, neither TMR nor TBK have reported any actual or attempted misuse of this information as a result of this incident.

Notice to Iowa Residents

On October 28, 2020, the City provided written notice of the TMR incident to five thousand three hundred eighty-seven (5387) 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

The City takes the confidentiality, privacy, and security of personal information very seriously. After receiving notice from TBK, the City took steps to understand the impact the TMR data security incident had on the City data. Upon confirmation of this information, the City worked to identify those individuals whose information was contained in the check images. As part of its ongoing commitment to the security of information, the City is reviewing its existing policies and procedures regarding our third-party vendors and is working with TBK to evaluate additional measures and safeguards to protect against this type of incident in the future. The City will also notify other government regulators, as required.

As noted above, the City is notifying potentially affected customers. This notice provides 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.

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

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/jc1

EXHIBIT A

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

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

<<Date>>

Dear <<Name 1>>:

The City of Bettendorf, IA ("The City") is writing to notify you because you may have been affected by the Technology Management Resources, Inc. ("TMR") data security incident. TBK Bank ("TBK"), the City's third-party treasury management services vendor, which includes utility payment processing, has an agreement with TMR to provide Lockbox Payment Processing services for TBK on behalf of the City. While there is currently no evidence that your information has been misused as a result of this incident, we are providing you with information on the event, measures we have taken, and what you may do to better protect your personal information should you feel it appropriate to do so.

What Happened? On August 27, 2020, the City received notice from TBK of the TMR data security incident. The notice indicated that an unauthorized actor had gained access to TMR's systems and, consequently, may have been able to access images of checks that were sent to TBK's Lockbox. TBK also provided a list of individuals associated with the City that TMR believed may have been affected by the incident. Upon receipt of the notice, the City immediately commenced an investigation to determine the nature and scope of the underlying event. On September 17, 2020, TBK confirmed that the unauthorized actor had access to the TMR systems from June 1, 2020, to July 1, 2020. TBK further confirmed that the actor may have gained access to images of checks relating to City customers on the TMR system.

What Information Was Involved? TMR's investigation confirmed that at the time of the incident the information present within the involved TMR systems included your name, checking account number, and routing number. To date, neither TMR nor TBK have reported any actual or attempted misuse of this information as a result of this incident, as it pertains or relates to the City.

What We Are Doing. We take the confidentiality, privacy, and security of personal information very seriously. After receiving notice from TBK, we took steps to understand the impact the TMR data security incident had on City data. Upon confirmation of this information, the City worked to identify those individuals whose information was contained in the check images. As part of our ongoing commitment to the security of information in our care, we are reviewing our existing policies and procedures regarding our third-party vendors, and are working with TBK to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying government regulators, as required.

What You Can Do. You may review the information contained in the enclosed "Steps You Can Take to Protect Your Personal Information." In addition, you can carefully monitor your checking account. If you see any unauthorized or suspicious activity, you can promptly contact your bank and/or credit union.

For More Information. We understand you may have questions about the TMR incident that are not addressed in this letter. For this incident, and to ensure your questions are answered in a timely manner, we established a dedicated assistance line at **833-364-1208** which can be reached Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. You may also contact the City by mail at 1609 State Street, Bettendorf, Iowa 52722

Sincerely,

Decker P. Ploehn

Decker Ploehn
City Administrator
City of Bettendorf, IA

Steps You Can Take to Protect Your Personal Information

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud. 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	TransUnion	Equifax
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Chester, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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	TransUnion	Equifax
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	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 Ave. NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), and 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, 1-410-528-8662, and 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 1-919-716-6000, and www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-788-9898, and www.ag.ny.gov/

For Washington, D.C. residents, the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, 1-202-442-9828, and https://oag.dc.gov.