City of Keene
New Hampshire

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

November 11, 2020

F9556-L01-0000001 T00017 P003 *********ALL FOR AADC 123
SAMPLE A SAMPLE - L01
APT B
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notice of Data Security Breach

Dear Keene Community Member,

We are writing to inform you about a security breach at Technology Management Resources, Inc. (TMR), which is a third-party vendor of Mascoma Bank (Mascoma Bank). The breach involves your personally identifiable information (PII). The information impacted by this event includes your name, address, and the account and routing numbers of your bank or financial account. As discussed further below, as a result of this breach, we encourage you to: (1) enroll in the identity, credit, and financial monitoring and remediation services discussed below; (2) contact your bank or financial institution to alert it about this breach; and (3) review the activity in your bank or financial account now and routinely thereafter, and notify your bank or financial institution immediately about any suspected fraud.

What Happened: Mascoma Bank is a bank that the City of Keene (City) uses to manage certain of the City's financial accounts. One function that Mascoma Bank performs is receiving, scanning, and depositing checks written and mailed to the City. Mascoma Bank recently informed the City that TMR, Mascoma Bank's data processing vendor, experienced a security breach. According to Mascoma Bank and TMR, an unauthorized individual gained access to TMR's database in June 2020. As a result, that individual was able to view the images of scanned checks written to the City between June 2019 and January 2020. You are receiving this notice because the database included a check or checks from you.

What Information Was Involved: An image of a scanned check includes both the routing number of your bank or financial institution, and the number of your account at that bank or financial institution. That information could be used to attempt to withdraw or transfer funds from your account. Additionally, an image of a scanned check also may include your signature, name, address, phone number, the number of the check, the amount of the check, any information you may have put on the memo line or other areas of the check, an example of your handwriting, and any other information that exists or that you put on your check.

At present, the City is not aware that your information has been misused. Nonetheless, we encourage you to take the below measures to protect yourself.

What You Should Do: Because an image of a check contains PII, you are being offered services to protect your identity, credit, and bank account. Specifically, you are being offered a complimentary two year membership in Experian IdentityWorks. This product provides you with identity and credit protection and resolution of identity, credit, and certain financial fraud. To activate your membership please follow these steps:

- Enroll by ***January 31, 2021***. Your code will not work after that date.
- Visit the Experian IdentityWorks website: https://www.experianidworks.com/credit
- Provide the following activation code: **ABCDEFGHI**

If you have questions about this service, or need assistance with identity, credit, or financial fraud restoration, please contact Experian at (866) 578-5413 by January 31, 2021. Please be prepared to provide engagement number DB23258 as proof of eligibility for the identity, credit, and financial fraud restoration services. A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any identity, credit, or financial fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup.
- Credit monitoring that actively monitors Experian file for indicators of fraud.
- Identity Restoration agents are immediately available to help you address any identity, credit, and financial fraud.
- Up to $1 million of identity theft insurance that provides coverage for certain costs and unauthorized electronic fund transfers.[1]

The City strongly encourages you to promptly use the foregoing information to enroll yourself in these credit, identity, and financial crime protection services.

In addition, because an image of a check includes the routing and account numbers, we encourage you to promptly contact your bank or financial institution and alert it about this breach. Your bank or financial institution may be able to offer you specific protections for your account. Additionally, you should promptly review the activity in your account for the past several months to determine if there is any potential fraud, and continue to monitor your account activity routinely thereafter, not less than monthly. If you suspect any fraud, you should inform your bank or financial institution immediately.

[1] Identity theft insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

What You Can Do: While this security breach did not involve your Social Security number or any of your governmental identification numbers, other measures you could take if you feel that you need to protect yourself are as follows: (1) obtain your credit reports from www.annualcreditreport.com, inspect them for any potentially fraudulent activity, and notify the creditor if fraudulent; and (2) either implement a 90-day fraud alert, or freeze/lock your files with each of the three major credit bureaus. You are entitled at this time to inspect your credit reports, implement a fraud alert, and freeze/lock your credit without charge to you. While the City does not feel that you need to take these steps to protect yourself with respect to this security breach, if you would like to do so, the following is the contact information for the three major credit bureaus:

Equifax	Experian	TransUnion
866-349-5191	888-397-3742	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Finally, Mascoma Bank has informed the City that TMR filed a report with the Federal Bureau of Investigation (FBI). The City is not aware that Mascoma Bank or TMR filed a report with any other police or law enforcement authority. Under certain state and federal laws, you may have a right to obtain a copy of such reports. If you wish to do so, you should contact the FBI. If you experienced financial or other crime as a result of the TMR breach, you should contact either the FBI or your state or local police.

What the City Is Doing: The City respects the privacy of your information. As a result, the City is working with a cybersecurity attorney to ensure that Mascoma Bank and any of its vendors that handle information for the City (including TMR) have implemented reasonable measures designed to safeguard the confidentiality of such information.

For More Information: If you do have any questions, please call (866) 578-5413 or inquiries@ci.keene.nh.us. The City apologizes for any inconvenience this situation causes. Thank you.

Sincerely,

Thomas P. Mullins,
City Attorney

0000001

F9556-L01

City of Keene
New Hampshire

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

November 11, 2020

F9556-L02-0000002 P003 T00017 *********ALL FOR AADC 123
SAMPLE COMPANY
APT B
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notice of Data Security Breach

Dear Keene Community Member,

We are writing to inform the organization named above about a security breach at Technology Management Resources, Inc. (TMR), which is a third-party vendor of Mascoma Bank (Mascoma Bank). The breach involved an image of a check that the organization sent to the City of Keene (City). That information includes the organization's name, address, and the account and routing numbers of its bank or financial account. As discussed further below, as a result of this breach, the City encourages the organization to: (1) enroll in the credit monitoring services discussed below; (2) contact the organization's bank or financial institution to alert it about this breach; and (3) review the activity in the organization's bank or financial account now and routinely thereafter, and notify its bank or financial institution immediately about any suspected fraud.

What Happened: Mascoma Bank is a bank that the City uses to manage certain of its financial accounts. One function that Mascoma Bank performs is receiving, scanning, and depositing checks written and mailed to the City. Mascoma Bank recently informed the City that TMR, Mascoma Bank's data processing vendor, experienced a security breach. According to Mascoma Bank and TMR, an unauthorized individual gained access to TMR's database in June 2020. As a result, that individual was able to view the images of scanned checks written to the City between June 2019 and January 2020. The organization named above is receiving this notice because the database included a check or checks from it.

What Information Was Involved: An image of a scanned check includes both the routing number of the organization's bank or financial institution, and the number of the organization's account at that bank or financial institution. That information could be used to attempt to withdraw or transfer funds from the organization's account. Additionally, an image of a scanned check also may include the organization's name, address, and phone number, the authorized signer for the organization, the number of the check, the amount of the check, any information that may have been put on the memo line or other areas of the check, an example of the check writer's handwriting, and any other information that exists or was placed on the check.

At present, the City is not aware that the organization's information has been misused. Nonetheless, we encourage the organization to take the below measures to protect itself.

What the Organization Should Do: Because an image of a check contains bank account and routing numbers, the organization is being offered services to protect its credit. Specifically, the organization is being offered a complimentary two year membership in Experian Business Credit Advantage. This product provides the organization with credit protection. To activate this membership please follow these steps:

- Enroll by ***January 31, 2021***. The code will not work after that date.
- Visit the Experian Business Credit Advantage website: www.smartbusinessreports.com/protectmycompany
- Provide the following activation code: **ABCDEFGHI**

If the organization has questions about this service, or needs assistance with credit monitoring, please contact Experian at (800) 303-1640 by **January 31, 2021**. Please be prepared to provide engagement number **ENGAGE#** as proof of eligibility for credit monitoring. A credit card is not required for enrollment in Experian Business Credit Advantage. The organization can contact Experian immediately regarding any credit issues, and has access to the following features once it enrolls in Business Credit Advantage:

- Monitoring of the organization's business credit file.
- Access to the organization's Experian business credit report.
- Email alerts of key changes indicating possible fraudulent activity.

The City strongly encourages the organization to promptly use the foregoing information to enroll itself in these credit protection services.

In addition, because an image of a check includes bank routing and account numbers, the City encourages the organization to promptly contact its bank or financial institution and alert it about this breach. The organization's bank or financial institution may be able to offer specific protections for the organization's account. Additionally, the organization should promptly review the activity in its account for the past several months to determine if there is any potential fraud, and continue to monitor activity in that account routinely thereafter, not less than monthly. If the organization suspects any fraud, the organization should inform its bank or financial institution immediately.

What the Organization Can Do: Other measures the organization could take if it decides that it needs to protect itself further are as follows: (1) obtain and/or monitor the organization's business credit reports at the agencies listed below, inspect them for any potentially fraudulent activity, and notify the agency and creditor if fraudulent; and (2) implement a fraud alert with Experian and Equifax, which are currently the only major credit bureau that implement fraud alerts for the accounts of organizations. While the City does not feel that the organization needs to take these steps to protect itself with respect to this security breach, if the organization would like to do so, the following is the contact information for the major credit bureaus:

Equifax
800-727-8495
www.equifaxsmallbusiness.com
P.O. Box 740241
Atlanta, GA 30374

Experian
888-397-3742
www.businesscreditfacts.com/pdp.aspx?pg=faq-fr2&lsv=www
P.O. Box 4500
Allen, TX 75013

TransUnion
800-888-4213
www.transunion.com
P.O. Box 740241
Atlanta, GA 30374

Dunn & Bradstreet
866-584-0283
www.dnb.com
P.O. Box 1000
Chester, PA 19016

Finally, Mascoma Bank has informed the City that TMR filed a report with the Federal Bureau of Investigation (FBI). The City is not aware that Mascoma Bank or TMR filed a report with any other police or law enforcement authority. Under certain state and federal laws, the organization may have a right to obtain a copy of such reports. If the organization wishes to do so, it should contact the FBI. If the organization experiences financial or other crime as a result of the TMR breach, the organization should contact either the FBI or the state or local police.

What the City Is Doing: The City respects the privacy of the organization's information. As a result, the City is working with a cybersecurity attorney to ensure that Mascoma Bank and any of its vendors that handle information for the City (including TMR) have implemented reasonable measures designed to safeguard the confidentiality of such information.

For More Information: If the organization has any questions, please call (866) 578-5413 or inquiries@ci.keene.nh.us. The City apologizes for any inconvenience this situation causes. Please be prepared to provide engagement number ENGAGE#. Thank you

Sincerely,

Thomas P. Mullins,
City Attorney

0000002

F9556-L02

Mascoma Bank

August 26, 2020

Re: Notice of Mascoma Bank Data Security Incident

Dear City of Keene,

Mascoma Bank is writing to notify you of a recent data security incident that may affect the security of information of certain of The City of Keene's residents. This information was provided to Mascoma Bank by our lockbox managed service provider.

What Happened? Mascoma Bank was recently notified by our lockbox provider Technology Management Resources, Inc. ("TMR") of a security incident that impacts certain resident information that TMR processes for us, on your behalf. TMR regularly collects the contents of your PO Box lockboxes and scans check images into an online database for processing. TMR's internal investigation of the incident showed that between June 1, 2020 through July 1, 2020, a single unauthorized actor accessed the TMR online database and was able to view scanned images of checks written by your residents for the period of August 2019 to January 2020. To date, we are unaware of fraudulent activity against your residents as a result of this incident. The information related to these individuals includes their name, address, bank routing number, and account number.

Under applicable law, The City of Keene may be required to provide notice of this incident to the affected residents as well as certain regulators. We are unable to provide you with legal advice and recommend you discuss the contents of this letter and your company's potential notification duties with your own legal counsel should you require specific legal guidance.

On behalf of The City of Keene, Mascoma Bank is offering to pay for your mailing of any written notice of this incident if you choose that path. Additionally, complimentary credit monitoring/identity theft protection services to your impacted consumers whom request protection due to sensitive information that may have been viewed by the unauthorized actor, to the extent address information exists for such consumers. We will also provide notification of this incident to our regulatory bodies.

We need to have further conversations about your approach on next steps in regard to this mailing and assist with resources regarding customer communication.

Mascoma Bank takes the privacy and security of the personal information in our care seriously and appreciate you being a customer. Please call Scott Young, at 603-443-8649 or scott.young@mascomabank.com with any questions or concerns.

Sincerely,

Scott Young, Chief Retail Officer
Mascoma Bank