Memo

To: **Certain** Town of Colchester Employees and **Certain** Volunteers who receive Stipends, who have been provided this memo in an individually addressed envelope
From: [redacted]
Date: January 19, 2022
Re: Update-Town of Colchester Digital Intrusion and Potential Data Security Incident

I am writing with an update on a data security incident that we alerted you to in December, to provide access to a credit monitoring and identity protection services, to let you know of steps you can take, and to apologize.

What Occurred: On Thursday, December 8, 2021, the Town of Colchester became aware that fraudulent emails were being sent from Town email accounts. We immediately started investigating what appeared to be a spam issue. On Friday, December 9, we asked all users to reset their email passwords based on information provided to us by our email service provider. On Monday December 13, the issues became more widespread and we became concerned it may be more than spam. We requested our email be shut down at that time. On Wednesday December 15, we moved our email to another email provider. It appears there was either a virus sending the fraudulent emails or some of our email accounts were accessed. Our investigation is ongoing and we do not yet have final conclusions as to the nature of the incident.

What Information Was Involved: At this stage, it appears that the perpetrators of the digital intrusion may have gained access to emails sent and received by Town employees, though we do not yet have forensic evidence of such access. Those emails may have included financial information such as employee payroll records, which may have exposed employee names, Social Security numbers, direct deposit bank account number, and—potentially—other personal identifiable information. If this memo was provided to you in an envelope addressed to you directly, your personal identifiable information may have been included in those impacted email accounts.

Next Steps: We are continuing to work with law enforcement, Town IT staff, the email provider, and outside IT vendors to understand the full extent of the digital intrusion and what information may have been impacted.

To protect you from potential misuse of your information, we are providing a three-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your three-year membership, please see the additional information provided in and attached to this memo.

This memo provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Please accept my apologies that this incident occurred. We remain committed to maintaining the privacy of personal information in our possession and have taken additional precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of personal information. Please feel free to call at [redacted] if you have any questions.

Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion LLC
P.O. Box 6790
Fullerton, PA 92834-6790
https://www.transunion.com/fraud-alerts
(800) 680-7289

Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.