From:
Sent: Friday, February 10, 2023 5:45 PM
To:
Subject: Notice of Inadvertently Disclosed Personal Information

On behalf of the Town of Brookline, I want you to know that we value your public service and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about an incident that involves your personal information.

What Happened? A current Town of Brookline employee filed a complaint with MCAD. As part of that claim, an MCAD investigator requested a copy of the employee's personnel folder. An employee of Town Counsel's Office complied with the request, but inadvertently included as part of the response, a document listing the other employees promoted at the same time as the employee/MCAD complainant.

You were one of those employees. These promotion forms included the names, home addresses, dates of birth, and social security numbers of several employees promoted at the same time.

The information was inadvertently sent to only two people—the current Town employee and the MCAD employee. What occurred is not like the news stories you may have read about where your personal information may now be all over the internet.

The current Town employee and the MCAD employee received the information on January 13, 2023. On January 25, we sent each recipient those same forms, but with your personal information redacted. We asked both the current Brookline employee and the MCAD employee to delete the inadvertently disclosed information.

Having not heard from them, I sent them another email today asking them to confirm that they deleted the inadvertently disclosed information and shared it with no one. I have yet to hear back from them.

What Information Was Involved? The data inadvertently disclosed included personal information such as names, home addresses, dates of birth, and social security numbers.

The data inadvertently disclosed ***did not include*** any other personal information, such as driver's license numbers, state-issued identification card numbers, bank account, financial account, credit card or debit card numbers, or any required security codes, access codes, personal identification numbers, or passwords required to access any accounts.

What Are We Doing? The Town of Brookline values greatly your privacy. On behalf of the Town, the entire Town Counsel's Office, and the employee who inadvertently disclosed the information, we apologize and deeply regret that this incident occurred.

The Town, Town Counsel's Office, and the Human Resources Department will continue to implement even better measures designed to prevent a recurrence of such an inadvertent disclosure and to protect the privacy of our valued employees, current and retired.

What Can You Do? There are many steps you can take to further protect yourself. You should be taking these steps regardless of this inadvertent disclosure.

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain as you have always been vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including the Massachusetts attorney general, the Norfolk district attorney, the Brookline Police Department, and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action.

Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

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 Atlanta, GA 30374	P.O. Box 2002 Allen, TX 75013	2 Baldwin Place P.O. Box 1000 Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the FTC's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://consumer.ftc.gov/identity-theft-and-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338).

A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Other Information. In some US states, you have the right to put a security freeze on your credit file. A security freeze, also known as a credit freeze, makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent.

As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency.

To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement.

There is no charge to request a security freeze or to remove a security freeze.

For further information and questions, please feel free to send me an email.

Sincerely,

Town Counsel
Town of Brookline
e: