BATH FITTER®

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

RE: Notice of Data Breach

Dear <<Full Name>>,

In the spirit of caution and care for the Bath Fitter family, I am writing to share that Bath Fitter has been the victim of a recent cyber security incident. On December 26, 2024 we sent an email to all current employees providing interim notice of the incident and making credit monitoring available. As a result of our investigation of the incident, which we recently completed, we learned that some former employees may also have been impacted by the incident. We are sending this letter to provide formal notification of the breach to all potentially impacted current and former employees now that our investigation is complete.

What Information Was Involved?

Since personnel files may have been affected, it is possible that the breach affected passport numbers, driver's licenses, social security numbers (in the United States) and social insurance numbers (in Canada), birth dates, **financial account numbers without any associated personal identification numbers (PINs) or passwords**, health and safety related information, direct pay authorizations, compensation-related information as well as onboarding information such as applications, resumés and background checks. If the personnel file contains information about disciplinary action, it may have been potentially breached as well.

What We Are Doing.

VPN services and remote access to our network were disabled as we built a new, separate network with limited access to our systems. We remain committed to further enhancing our security measures as necessary to reduce the chances of future incidents.

IN ORDER TO HELP YOU PROTECT YOUR PERSONAL INFORMATION AGAINST IDENTITY THEFT AND OTHER TYPES OF FRAUD, WE HAVE MADE ARRANGEMENTS WITH CYEX, A GLOBAL LEADER IN IDENTITY MONITORING SERVICES. CYEX'S CREDIT MONITORING SERVICES WILL BE AVAILABLE TO YOU, AT NO COST, FOR A PERIOD OF TWO (2) YEARS FROM YOUR ENROLLMENT DATE. WE STRONGLY ENCOURAGE YOU TO CONSIDER ENROLLING. TO ENROLL PLEASE CONTACT 855-295-4790 WITHIN 3 MONTHS OF RECEIVING THIS LETTER.

What You Can Do.

Also, as a precaution, we strongly recommend that you promptly contact your credit card, insurance, financial and bank institutions, immediately change your passwords and follow any recommendations they may provide.

If you have not already done so, we ask you to change all of your passwords, both for the company, and any that you may have saved on files on the company's network.

Please take note of the following key reminders for passwords:

- Never use your bathfitter.com email address as a username for 3rd party websites (Ticketmaster, Amazon, etc..).
- Do not use the same password you have for your Bath Fitter account as for 3rd party websites.
- Use unique passwords for each of your personal accounts.
- Ensure your passwords are alphanumeric with special characters and at least 8 characters long.
- Use a password vault to safely keep inventory of your different usernames and passwords.
- Use multi-factor authentication (MFA), especially for accounts with sensitive/personal information.
- Make it a habit to change your passwords periodically - experts recommend at least every 3 months.
- Do not disclose, share, or reuse your passwords.

In addition, please be vigilant to avoid falling victim to phishing attempts. "Phishing" refers to the use of a deceptive message, the "phish", whether email, SMS/text message (known as smishing), phone call (known as vishing), social media message, or suspicious hyperlink that looks legitimate and encourages you to take actions that could compromise your computer, mobile device, or network, by encouraging you to reveal sensitive information.

Scammers use phishing attacks to steal valuable information and gain illegal access to systems. The email or message may also request personal information like account numbers or passwords.

Phishing emails and messages may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual such as CEOs or other company executives.

This is how you can avoid falling victim of a phishing attempt:

- Don't blindly trust anything that comes into your inbox. Always verify an email's authenticity before you click any links or open attachments. The same applies to SMS / text messages received on your mobile devices (phones, tablets, watches, etc.).
- Be suspicious of messages that are vague, generic, or impersonal, or that stir strong emotions, such as fear, empathy, urgency, or anger.
- Never trust an email that asks for personal or sensitive information, such as your username, password or financial information.
- Check the "From:" field closely, but keep in mind that this information can be spoofed.
- Phishing websites may look legitimate by imitating company logos and using domain names and URLs that might be close misspellings or lookalikes.
- If you suspect you've received a phish— report it using the Report Phish Alert button in your email or advise our IT Security team right away.
- Remaining vigilant helps protect Bath Fitter, our workspaces, and our people.

Please be advised that you can obtain more information about identity theft, fraud alerts and security freezes by contacting the Federal Trade Commission and/or the Attorney General's office in your home state, as well as any of the three nationwide consumer reporting agencies. You may also visit the website of the Federal Trade Commission to learn more about your rights under the Fair Credit Reporting Act (15 U.S.C. §§ 1681-1681x) at

https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act.

We encourage you to continue remaining vigilant over the next twelve to twenty-four months and review account statements regularly. You may also periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted. Remember to promptly report any suspicious activity or incidents of suspected identify theft to local law enforcement or the Massachusetts state Attorney General.

Credit Monitoring and Credit Freeze Instructions:

Credit Monitoring. As mentioned above, we are offering you two years of free credit monitoring from your enrollment date. Through credit monitoring, CyEx will track your credit report and credit score to identify any irregularity as well as provide you real time alerts and identify theft protection.

TO OBTAIN CYEX'S 24-MONTH FREE CREDIT MONITORING, PLEASE CONTACT WITHIN 3 MONTHS OF RECEIVING THIS LETTER OUR CALL CENTER AT 855-295-4790, WHICH IS AVAILABLE MONDAY TO FRIDAY, FROM 9:00 A.M. TO 9:00 P.M. EASTERN STANDARD TIME.

Credit Freeze. For employees in Québec and in the United States, the law allows you to place security freezes on your credit report. The security freeze prohibits the credit assessment company holding your credit report from communicating it where the communication is for the purpose of entering into a credit related contract. This avoids impersonators opening a new account in your name.

You may contact the credit reporting agencies:

- In the U.S.:
  Equifax, PO Box 74021, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

  Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

  TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

- In Canada:

  Equifax, National Consumer Relations, Box 190, Montreal, Quebec, H1S 2Z2, www.equifax.ca, 1-800-465-7166
  TransUnion, Consumer Relations Department, P.O. Box 338, LCD1, Hamilton, Ontario L8L 7W2, www.transunion.ca, 1-800-663-9980.

  Please note that in Canada you have to contact both.

For More Information

We are sorry for any inconvenience or concern this may have caused you. For additional information about how the breach may have affected you, please contact WITHIN 3 MONTHS OF RECEIVING THIS LETTER our call center at 855-295-4790, which is available Monday to Friday, from 9:00 a.m. to 9:00 p.m. Eastern Standard Time.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

BATH FITTER

Your Operations Support Team

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 74021, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.
To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.
You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, PO Box 105281, Atlanta, GA 30348-5281.

> **Depending on the state you reside in**, you may obtain one or more additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaints with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it, or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Massachusetts residents: You have the right to file and obtain a copy of a police report. You also have the right to request a security freeze at no charge (see above). You may contact and obtain information from and/or report identity theft to your state attorney general at the Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, www.mass.gov/ago, 1-617-727-8400.

Fair Credit Reporting Act. You also have rights under the Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act). The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting agencies is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting agency. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.

- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.