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

To Whom It May Concern:

We are writing to inform you that a criminal actor gained unauthorized access to Bath Fitter's system, resulting in a data security incident at Bath Fitter ("we", "us", or "our"). Bath Fitter is a wholly-owned subsidiary of Bath Fitter Manufacturing Inc, which is wholly-owned by Bath Fitter Holdings Inc. The incident may have involved your personal information, and this letter provides details about what happened, what information of yours may have been involved, and what resources are available to you.

What Information Was Involved?

Based on the investigation to date, the incident may have affected certain personal information relating to you. This may include your social security number, date of birth, financial account numbers (without any associated personal identification numbers (PINs) or passwords), health and safety information, direct pay authorizations, compensation-related information, and onboarding materials such as applications, résumés, background checks, and records related to disciplinary actions. If you provided a passport or driver's license number during your employment, this information may also have been impacted.

What We Are Doing.

Upon discovering the incident, we immediately launched a thorough investigation with the support of a leading cybersecurity firm. We also conducted an internal analysis to determine what data was impacted. This notice has not been delayed as a result of a law enforcement investigation.

We are making credit monitoring available through Epiq for a period of twenty-four (24) months at no cost to you. You can enroll using the instructions below.

To protect against future security incidents, we have taken a number of steps, including:

- Engaging a dedicated Security Operations Center (SOC) to provide continuous, around-the-clock monitoring of our systems and network for suspicious activity and potential threats;
- Implementing multi-factor authentication (MFA) across our systems to add an additional layer of security to user accounts and reduce the risk of unauthorized access;
- Replacing our existing endpoint protection solution with an enhanced platform that provides stronger detection and response capabilities against cyber threats; and

- Making targeted adjustments to our network infrastructure to strengthen our overall security posture, including enhanced segmentation, improved access controls, and updated firewall configurations.

What You Can Do.

If your personal information has been accessed, you may be at heightened risk of fraud or identity theft. Therefore, we recommend that if you discover any suspicious or unusual activity on your accounts, your credit reports, or your online accounts, you promptly notify the financial institution or company with which your account is maintained.

Steps you can take to protect your identity include:

- Enroll in the offered credit monitoring service;
- Review account statements, explanation-of-benefits statements, and credit reports for suspicious activity;
- Report suspected identity theft or fraud promptly to financial institutions, insurers, local law enforcement, your state Attorney General, and the Federal Trade Commission;
- Consider placing a fraud alert or security freeze on your credit file as explained below;
    - A fraud alert tells creditors to take extra steps to verify your identity before extending credit. An initial fraud alert lasts one year and can be placed by contacting any one of the three major credit reporting agencies listed below. That agency will notify the other two.
    - A security freeze restricts access to your credit report, making it more difficult for identity thieves to open new accounts in your name. There is no charge to place, temporarily lift, or permanently remove a security freeze. To place a freeze, contact each of the three credit reporting agencies directly using the contact information listed below. You may need to provide name, SSN, date of birth, address, proof of residency, and proof of identity to place a security freeze; and
- You have the right to file a police report if you believe you are the victim of identity theft. You may also obtain information from law enforcement about identity theft crimes.

For More Information.

We apologize for any inconvenience or concern this may have caused you. For additional information about how the breach may have affected you, please contact our call center at 1-888-616-9421, which is available Monday through Friday, 9 am to 9 pm Eastern Time (excluding US holidays).

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

Sincerely,

BATH FITTER
Your Operations Support Team

ADDITIONAL RESOURCES

The following resources may be helpful to potentially affected individuals:

Resource	Contact information
Free credit reports	www.annualcreditreport.com | 1-877-322-8228
Identity theft recovery assistance	www.IdentityTheft.gov | 1-877-438-4338
Fraud alerts and security freezes	**Equifax:** P.O. Box 740241, Atlanta, GA 30374, 1-800-685-1111, www.equifax.com/personal/credit-report-services; **Experian:** P.O. Box 4500, Allen, TX 75013, 1-888-397-3742, www.experian.com; **TransUnion:** P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com

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.IdentityTheft.gov, 1-877-438-4338. You may also contact your local state Attorney General.

- **For Massachusetts residents:** You may contact the Office of the Attorney General, Consumer Advocacy and Response Division, 1 Ashburton Place, 20th Floor, Boston, MA 02108, https://www.mass.gov/info-details/consumer-services-at-the-attorney-generals-office, 1-800-697-1220.

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 are 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.

Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: 24 Months

Epiq - Privacy Solutions ID
3B Credit Monitoring

How To Enroll:

1) Visit www.privacysolutionsid.com and click "Activate Account"
2) Enter the following activation code, **<<Activation Code>>** and complete the enrollment form
3) Complete the identity verification process
4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5) Enter your log-in credentials
6) You will be directed to your dashboard and activation is complete!

Product Features:

3-Bureau Credit Monitoring with Alerts
Monitors your credit file(s) with each of the 3 Credit Bureaus for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score with Score Tracker[1]
1-Bureau VantageScore®3.0 (monthly) and Credit Score Tracker.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)
Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring
Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring
Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Credit Protection
3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Personal Info Protection
Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance
Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to $1M Identity Theft Insurance[2]
Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT[2]
Provides up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 3B Credit Monitoring, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

1 The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

2 Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.