

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: 1.410.456.2741
Cell: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

January 19, 2024

VIA EMAIL or EMAIL

Anthony Brown
Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Newington Fire Department – Incident Notification

Dear Anthony Brown:

McDonald Hopkins PLC represents Newington Fire Department (“Newington FD”) located at 80 Fox Point Road, Newington, New Hampshire 03801. I write to provide notification concerning an incident that may affect the security of personal information of one (1) Maryland resident. By providing this notice, Newington FD does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction

Newington FD detected unauthorized access to certain systems on its network due to a network security incident. Upon learning of this issue, Newington FD immediately initiated an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations. Based on its comprehensive investigation, Newington FD determined that an unauthorized party potentially accessed and removed files from the network on September 22, 2023. After an extensive forensic investigation, Newington FD began a comprehensive manual review of the impacted files. On December 26, 2023, Newington FD discovered that certain files containing personal information were potentially removed from its network in connection with this incident, including the affected residents’ full names and Social Security numbers.

To date, Newington FD is not aware of any reports of identity theft or financial fraud as a direct result of this incident. Nevertheless, out of an abundance of caution, Newington FD wanted to make you (and the affected resident) aware of the incident and explain the steps that it is taking to safeguard the resident against potential misuse of their information. Newington FD is providing notice to the affected resident commencing on or about January 19th, 2024 in substantially the same form as the document attached hereto as **Exhibit A**. Newington FD is also offering complimentary credit monitoring to the impacted resident. Additionally, Newington FD is advising the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or

irregular activity on a regular basis. The resident is also being provided with best practices to protect personal information, such as placing a fraud alert and/or security freeze on their credit files and obtaining a free credit report. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Newington FD, protecting the privacy of personal information is a top priority. Newington FD is committed to maintaining the privacy of employee information and is continually evaluating and modifying its practices and procedures to enhance appropriate and privacy measures to prevent recurrence of this incident.

If you have any additional questions, please contact me at (410) 456-2741 or spollock@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Spencer S. Pollock", with a stylized flourish at the end.

Spencer S. Pollock

Encl.

Exhibit A



**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

Dear [REDACTED]

I am writing with important information regarding a recent data security incident that may have impacted your personal information. The privacy and security of the personal information we maintain is of the utmost importance to the Newington Fire Department ("Newington FD"). With this notice, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

We learned certain systems in Newington FD's network environment were affected by a cybersecurity incident.

What We Are Doing.

Upon learning of the issue, we immediately secured the network environment, notified law enforcement, and launched an investigation in consultation with outside cybersecurity professionals who regularly investigate these types of incidents to analyze the extent of any unauthorized activity in Newington FD's network environment. After an extensive forensic investigation and document review, we determined on December 26, 2023 that your personal information may have been accessed or acquired by an unauthorized party on or about September 22, 2023.

What Information Was Involved?

The potentially involved information includes your full [REDACTED]

What You Can Do?

We have no evidence that any of your information has been used for identity theft or financial fraud as a result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To help protect you from potential misuse of your information, we are offering a complimentary 12 month membership with Experian IdentityWorksSM. 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. Experian IdentityWorks is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks, including instructions

on how to activate your complimentary membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures to protect your personal information, including placing a fraud alert, placing a security freeze, and/or 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.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. **If you have any further questions regarding this incident, please contact us at [REDACTED].** We will contact you within a timely manner.

Sincerely,

Newington Fire Department

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary Credit Monitoring**

1. ENROLL by: [REDACTED] (Your code will not work after this date.)
2. VISIT the Experian IdentityWorks Website to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the Activation Code: [REDACTED].

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.890.9332. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS CREDIT 1B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll** in the product regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877-288-8057 to register with the activation code above.**

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

2. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the credit monitoring services, we recommend that you place an initial 1-year “fraud alert” on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. 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. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<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

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

Following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below). You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

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

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting 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 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.

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.

4. 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.

5. 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 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.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.