McDonald Hopkins
A business advisory and advocacy law firm®

RECEIVED
APR 06 2026
CONSUMER PROTECTION

McDonald Hopkins LLC
300 N. LaSalle Street
Suite 1400
Chicago, IL 60654

P 1.312.280.0111
F 1.312.280.8232

Nicholas A. Kurk
Direct Dial: 312-642-6738
E-mail: nkurk@mcdonaldhopkins.com

April 1, 2026

VIA U.S. MAIL

The Hon. John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Town of Amherst– Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Town of Amherst, located at 2 Main Street, Amherst, New Hampshire 03031. I am writing to provide notification of a potential security incident at the Town of Amherst that may affect the security of personal information of approximately two hundred and sixty (260) New Hampshire residents. By providing this notice, Town of Amherst does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

The Town of Amherst recently learned that, on or about February 3, 2026, several employees had issues related to tax filings. Upon learning of the issue, the Town of Amherst immediately secured our network and conducted a thorough investigation. As part of its investigation, the Town of Amherst engaged leading cybersecurity experts to identify what personal information, if any, was involved. The Town of Amherst's investigation is still ongoing. At this time, there is no evidence to indicate that there was any compromise to the Town of Amherst's systems or network. However, out of an abundance of caution and because the Town of Amherst cannot rule out the possibility that personal information was impacted, the Town of Amherst wanted to notify all potentially impacted individuals. It is believed that the files potentially impacted contained personal information pertaining to a limited number of individuals, such as full names and social security numbers.

Out of an abundance of caution, the Town of Amherst wanted to inform you of the incident and to explain the steps it is taking to help safeguard the affected residents against identity fraud. Town of Amherst provided the affected residents with notification of this incident commencing on or about April 1, 2026 in substantially the same form as the letter attached hereto as **Exhibit A**. Town of Amherst advised the affected individuals to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. The affected individuals were also provided with contact information for the consumer reporting agencies and the Federal Trade Commission. Individuals whose Social Security numbers were involved will be provided with a complimentary one-year membership with a credit monitoring service upon request.

At Town of Amherst, protecting the privacy of personal information is a top priority. Town of Amherst is committed to maintaining the privacy of personal in its possession and has taken many

precautions to safeguard it. Town of Amherst continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (312) 642-6738 or nkurk@mcdonaldhopkins.com.

Very truly yours,

Nicholas A. Kurk

Return Mail Processing
PO Box 999
Suwanee, GA 30024

1 1 270 **********SNGLP
[redacted]

April 1, 2026

[redacted]

[redacted]

The privacy and security of the personal information we maintain is of the utmost importance to the Town of Amherst. We are writing to provide you with information regarding a potential cybersecurity incident that may have involved your personal information. Please read this notice carefully, as it provides information about the incident, the complimentary identity monitoring services we are making available to you, and precautionary measures you can take to protect your information.

What Happened?
On or about February 3, 2026, the Town of Amherst learned that several employees had issues related to tax filings.

What We Are Doing.
Upon learning of the issue, we secured our network and commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Our investigation is still ongoing. At this time, we have no evidence to indicate that there was any compromise to our systems or our network. However, out of an abundance of caution and because we cannot rule out the possibility that your information was impacted, we wanted to make you aware of the incident.

What Information Was Involved?
The information that may have been impacted would be your W-2 tax form, which includes your first and last name and [redacted].

What You Can Do.
As explained above, we want to make you aware of the incident and provide complimentary credit monitoring services as a precaution. We are providing you with complimentary access to Experian IdentityWorks℠ for [Extra1] months. This letter provides more information about the complimentary services, enrollment instructions, and other precautionary measures you can take to protect your personal information, including reporting fraud affecting your tax records to the IRS, 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.

For More Information.
If you have questions, please contact our dedicated and confidential call center at [redacted]. The response line is available for 90 days from the date of this letter, between the hours of 9 am to 9 pm Eastern time, Monday through Friday, excluding holidays. We apologize for any inconvenience or concern this may cause. We have taken this matter very seriously and will continue to take significant measures to protect the personal information in our possession.

Sincerely,

Town of Amherst

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary Credit Monitoring.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for [redacted] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [redacted] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [redacted]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** July 31, 2026 by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [redacted]
- Provide your **activation code:** [redacted]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by July 31, 2026 at 833-918-3959, Monday - Friday, 9 am - 9 pm Eastern Time (excluding major U.S. holidays). Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [redacted]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE[TM]:** 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.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert.

We recommend that you place a one-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
Equifax Information Services LLC
P.O. Box 105069, Atlanta, GA 30348-5069
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
1-888-EQUIFAX (1-888-378-4329)

Experian
P.O. Box 9532, Allen, TX 75013
www.experian.com/fraud
1-888-EXPERIAN (1-888-397-3742)

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000, Chester, PA 19016
www.transunion.com/fraud-alerts
800-916-8800; 800-680-7289

3. Consider 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 cost. 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, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
Equifax Information Services LLC
P.O. Box 105788, Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-888-EQUIFAX (1-888-378-4329)

Experian Security Freeze
P.O. Box 9554, Allen, TX 75013
www.experian.com/freeze
1-888-EXPERIAN (1-888-397-3742)

TransUnion Security Freeze
P.O. Box 160, Woodlyn, PA 19094
www.transunion.com/credit-freeze
800-916-8800; 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 such as copy of a government issued identification. 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 you do place a security freeze prior to enrolling in a credit monitoring service, 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. Reporting Identity Fraud to the IRS.

If you believe you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended you do the following:

- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf.
- Call the IRS at (800) 908-4490, ext. 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police or law enforcement department.

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

You may also request an Identity Protection PIN (IP PIN) from the IRS at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. An identity protection PIN (IP PIN) is a six-digit number that prevents someone else from filing a tax return using your Social Security number (SSN) or individual taxpayer identification number (ITIN). The IP PIN is known only to you and the IRS. It helps us verify your identity when you file your electronic or paper tax return.

6. 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.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.