McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

February 12, 2021

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Town of Amherst – Incident Notification

Dear Attorney General MacDonald :

McDonald Hopkins PLC represents the Town of Amherst. I am writing to provide notification of an incident at the Town of Amherst that may affect the security of personal information of two (2) New Hampshire residents. The Town of Amherst's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, the Town of Amherst does not waive any rights or defenses.

On January 20, 2021 the Town of Amherst discovered that two DD214 forms and veteran exemption application forms, were inadvertently made publicly available online from January 15, 2021 to January 20, 2021 as part of the Town of Amherst's Board of Selectman Meeting Agenda. As soon as the Town of Amherst learned of the incident they immediately took the forms offline and began a thorough investigation of the incident. The information impacted included the affected residents' full names, Social Security numbers, and dates of birth.

Shortly after the Town of Amherst became aware of the incident, they personally contacted the two (2) impacted New Hampshire residents to discuss what happened. The Town of Amherst verbally advised the individuals of the incident and informed them that they would be reimbursed for their purchase of twelve (12) months of LifeLock credit monitoring and identity theft protection services.

The Town of Amherst has no evidence that any of the information has been misused. Out of an abundance of caution, the Town of Amherst wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the impacted residents against identity fraud. In addition to verbally advising the individuals of the incident, the Town of Amherst is also providing the affected residents with written notification of this incident commencing on or about February 12, 2021 in substantially the same form as the letter attached

hereto. The Town of Amherst is reimbursing the residents for twelve (12) months of credit monitoring and is advising the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. The Town of Amherst is advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At the Town of Amherst, protecting the privacy of personal information is a top priority. The Town of Amherst is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. The Town of Amherst continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

James J. Giszczak

Encl.

TOWN OF AMHERST, NH

Town Administrator
Dean E. Shankle, Jr., Ph.D.
dshankle@amherstnh.gov

2 Main Street
Amherst, NH 03031
(603) 673-6041

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

Dear [redacted]

The privacy and security of the personal information we maintain is of the utmost importance to the Town of Amherst. As you know, we contacted you regarding a data security incident on January 20, 2021. We are writing with additional important information regarding the data security incident that involved some of your information. We want to provide you with additional information about the incident, explain the services we will be reimbursing you for, and let you know that we continue to take significant measures to protect your information.

What Happened?

As you know, on January 20, 2021 we discovered that your DD214 form and your Application for Property Tax Exemption were inadvertently made publicly available online from January 15, 2021 to January 20, 2021 as part of the Town of Amherst Board of Selectman Meeting Agenda. As soon as we learned of the incident we immediately took the forms offline.

What We Are Doing.

Upon learning of this issue, we immediately commenced a thorough investigation and contacted you regarding this inadvertent posting. As part of our investigation, we have worked very closely with external cybersecurity professionals. We have also taken several steps to implement additional technical safeguards internally to prevent the recurrence of similar incidents.

What Information Was Involved.

The DD214 form and/or the Application for Property Tax Exemption contained some of your personal information, including your name, Social Security number, date of birth, phone number, branch of service, location of service, dates of services, blood type, home address and spouse name and phone number.

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we wanted to make you aware of the incident. To further help protect your information, we are reimbursing you for your purchase of a one-year membership of LifeLock to provide you with identity theft and credit monitoring protection. Once you have an invoice or receipt, please send them (a scanned copy will be sufficient) to me and I will process your payment.

For More Information.

Please accept our apologies that this incident occurred. We have taken necessary steps to prevent this from happening again. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it and to prevent subsequent occurrences. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call me at [redacted] Monday through Friday, 8:00 a.m. to 4:00 p.m. EST.

Sincerely,

[redacted]

Town of Amherst

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial one (1) 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	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

2. 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 charge. 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 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	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you'll 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.

3. 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.

4. 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.