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

Blair L. Dawson, JD, MS CyS, FIP, CIPP/US, CIPP/E, CIPM
Direct Dial: (312) 642-6131
E-mail: bdawson@mcdonaldhopkins.com

January 2, 2026

VIA U.S. MAIL

Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Gorlick, Kravitz, & Listhaus, P.C. – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents the Gorlick, Kravitz, & Listhaus, P.C. ("GKL"). I am writing to provide notification of an incident at GKL that may affect the security of personal information of approximately one (1) New Hampshire resident. By providing this notice, GKL does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On or about September 30, 2025 GKL learned that an unauthorized actor gained access to our network environment. Upon learning of this issue, GKL immediately began efforts to remediate the issue and commenced a prompt and thorough investigation. As part of our investigation, we have been working closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on December 3, 2025 that some personal information was contained in the impacted data that was accessed by the unauthorized actor on or around September 30, 2025. The information impacted included individuals' name and Social Security number.

GKL wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. GKL is providing the affected resident with written notification of this incident commencing on or about January 2, 2026 in substantially the same form as the letter attached hereto. GKL is offering the resident with Social Security numbers impacted a complimentary one-year membership with a credit monitoring service. Additionally, GKL has advised the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. The resident was also 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 were also provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At GKL, protecting the privacy of personal information is a top priority. GKL is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. GKL 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) 642-6131 or bdawson@mcdonaldhopkins.com.

Very truly yours,

Blair Dawson

Encl.

Gorlick, Kravitz, & Listhaus, P.C.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

[redacted]

Dear [redacted],

The privacy and security of the personal information we maintain is of the utmost importance to Gorlick, Kravitz, & Listhaus, P.C. ("GKL). We are writing with important information regarding a data security incident that may have involved some of your information. We want 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?

As a result of a cybersecurity incident, GKL learned that an unauthorized actor gained access to our network environment.

What We Are Doing.

Upon learning of this issue, GKL immediately began efforts to remediate the issue and commenced a prompt and thorough investigation. As part of our investigation, we have been working closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on December 3, 2025 that some of your personal information was contained in the impacted data that was accessed by the unauthorized actor on or around September 30, 2025.

What Information Was Involved?

This impacted data contained some of your personal and/or protected health information, including [redacted]

What You Can Do.

We have no indication that your information has been misused for identity theft. Out of an abundance of caution, however, we are offering a complimentary [redacted] months membership of identity theft protection services through Cyberscout, a Transunion company.

This letter also provides other precautionary measures you can take to protect your information, including placing a fraud alert and/or security freeze on your credit files, 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.

We are committed to maintaining the privacy of personal and protected health 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 information.

If you have any further questions regarding this incident, please call our toll-free response line at [redacted] The response line is available Monday through Friday, between the hours of 8 am and 8 pm EST.

Sincerely,

Gorlick, Kravitz, & Listhaus, P.C.
29 Broadway, 20th Floor
New York, New York 10006

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [redacted] -Month Credit Monitoring.

To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 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	*Experian*	*TransUnion*
P.O. Box 105069	P.O. Box 9554	Fraud Victim Assistance Department
Atlanta, GA 30348-5069	Allen, TX 75013	P.O. Box 2000
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	https://www.experian.com/fraud/center.html	Chester, PA 19016-2000
(800) 525-6285	(888) 397-3742	https://www.transunion.com/fraud-alerts
		(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 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*
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348-5788	Allen, TX 75013	Woodlyn, PA 19094
https://www.equifax.com/personal/credit-report-services/credit-freeze/	http://experian.com/freeze	https://www.transunion.com/credit-freeze
(888) 298-0045	(888) 397-3742	(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.

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 this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

****

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, Telephone: 888-743-0023.

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.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

There was 1 Rhode Island resident(s) impacted by this incident.