McDonald Hopkins
A business advisory and advocacy law firm®

100 International Drive
23rd Floor
Baltimore, MD 21202

P: 1.410.917.5189

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

June 25, 2026

VIA U.S. MAIL:

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Vision 3 Architects, Inc. – Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents Vision 3 Architects, Inc. ("V3") located at 317 Iron Horse Way, Suite 111, Providence, RI 02908. I am writing to provide notification of an incident at V3 that may affect the security of personal information of approximately two (2) New Hampshire residents. By providing this notice, V3 does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On or about April 24, 2026, V3 experienced unauthorized access to its network. Upon detecting the unauthorized activity, V3 immediately contained the incident and commenced a thorough investigation. As part of its investigation, V3 engaged leading cybersecurity experts to identify what personal information, if any, was involved.

After an extensive forensic investigation and manual document review, V3 discovered on or about May 27, 2026, that on or about April 24, 2026 certain files may have been subject to unauthorized access or acquisition containing personal information pertaining to a limited number of New Hampshire residents. The information included full names and Social Security numbers.

V3 is not aware of any reports of identity theft or financial fraud related to this incident. Nevertheless, out of an abundance of caution, V3 wanted to inform your office (and the affected residents) of the incident. V3 is providing the affected residents with written notification of this incident commencing on or about June 25, 2026 in substantially the same form as the letter attached hereto.

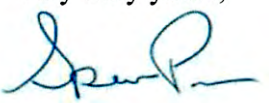
Notified individuals will be provided with best practices to protect their information. V3 will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. V3 will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. V3 will provide credit monitoring to individuals whose Social

Security number was potentially impacted. The affected residents are also being provided with the contact information for the consumer reporting agencies, and the Federal Trade Commission.

At V3, protecting the privacy of personal information is a top priority. V3 is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. V3 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 410.917.5189 or spollock@mcdonaldhopkins.com.

Very truly yours,



Spencer S. Pollock

Encl.

VISION 3
ARCHITECTS

[redacted]

[redacted]

[redacted]

Dear [redacted]:

We are writing with important information regarding a recent data security incident at Vision 3 Architects, Inc. involving some of your personal information. The privacy and security of the information we maintain is of the utmost importance to Vision 3 Architects, Inc. 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?

On or about April 24, 2026, we experienced unauthorized access to our network.

What We Are Doing.

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on May 27, 2026, that on April 24, 2026 certain files containing your personal information may have been subject to unauthorized access or acquisition. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

The information potentially impacted includes your [redacted].

What You Can Do.

We have no evidence of any identity theft or financial fraud related to this incident. Out of an abundance of caution to help protect your identity, we are offering a complimentary [redacted] month membership of Identity Monitoring services. For more information on identity theft prevention and Identity Monitoring services , including instructions on how to activate the complimentary [redacted] month membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal 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. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information on the following pages.

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 call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information. The response line is available Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

Vision 3 Architects, Inc.
317 Iron Horse Way, Suite 111
Providence, RI 02908

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [redacted] months Credit Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for [redacted] months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until [redacted] *to activate your identity monitoring services.*

Membership Number: [redacted]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

2. Placing a Fraud Alert.

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 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	*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 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. Protecting Your Medical Information.

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company.
- Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary.
- Follow up with your insurance company or the care provider for any items you do not recognize.

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.

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.

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.

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.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

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.

There were [redacted] Rhode Island residents impacted by this incident.