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

August 26, 2022

VIA EMAIL (DOJ-CPB@doj.nh.gov)

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

Re: Sewell & Neal, PLLC – Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents Sewell & Neal PLLC ("Sewell & Neal"), located at 220 West Main Street, Suite 1800, Louisville, KY 40202. I am writing to provide notification of an incident at Sewell that may affect the security of personal information of eight (8) New Hampshire residents. By providing this notice, Sewell does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On November 22, 2021 Sewell & Neal learned it was the victim of a cyberattack that caused encryption of certain files stored on its network. In addition to encrypting files, an unauthorized party removed a limited number of files from its system. Upon learning of the issue, Sewell & Neal commenced an immediate and thorough investigation and alerted law enforcement. As part of its investigation, Sewell engaged leading third-party experts experienced in handling these types of incidents. The investigation worked to identify what personal information, if any, might have been present in the removed files.

After an extensive forensic investigation and manual document review, Sewell & Neal discovered on July 29, 2022 that one or more of the files removed by the unauthorized party or about November 22, 2021 contained personally identifiable information such as full names, addresses, Social Security numbers, driver's license/state identification numbers, medical diagnosis and conditions information, health insurance information, financial account information, and/or payment card information.

Sewell & Neal provided the affected residents with written notification of this incident commencing on or about August 26, 2022, in substantially the same form as the letter attached hereto.

Sewell & Neal has no forensic evidence that any information has been actually misused or that there has been any fraud as a result of this incident. However, out of an

abundance of caution, Sewell & Neal wanted to inform your Office (and the affected residents) of the incident. Notified individuals have been provided with best practices to protect their information, including but not limited to complimentary credit monitoring services which were provided to those patients whose Social Security numbers may have been impacted by this incident.

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

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

Very truly yours,

James J. Giszczak

Encl.

SEWELL & NEAL, PLLC
ATTORNEYS AT LAW sonlegal.com
220 W. Main Street, Suite 1800, LG&E Center, Louisville, KY 40202 T: 502-582-2030 F: 502-561-0766
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
[redacted]
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [redacted]

[redacted]

[redacted]

August 22, 2022

Dear [redacted]

The privacy and security of the personal information we maintain is of the utmost importance to Sewell & Neal PLLC ("Sewell"). We are writing with important information regarding a recent data security incident that involved some of your information. We want to provide you with information about the incident, inform you about the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On November 22, 2021, Sewell detected unauthorized access to our network.

What We Are Doing.

Upon learning of this issue, we contained the threat by disabling all unauthorized access to our network and immediately 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 to analyze the extent of any compromise of the information on our network. After an extensive forensic investigation and manual document review, we discovered on July 29, 2022 that between November 9, 2021 and November 23, 2021 certain files containing your personal information may have been accessed and potentially acquired by an unauthorized individual(s).

What Information Was Involved.

The impacted files contained your personal information, specifically your name [redacted]

What You Can Do.

We have no evidence that any of your information has been misused. To protect you from potential misuse of your information, we are offering a complimentary [redacted] months membership of identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: [redacted] months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on your complimentary [redacted] months membership, please see the additional information provided in this letter.

This letter also provides precautionary measures you can take to protect your personal information, including 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.

Please accept our apologies that this incident occurred. We remain fully 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 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 protect against misuse of your information. The response line is available Monday through Friday, 9AM to 9PM Eastern.

Sincerely,

[redacted]

Sewell & Neal PLLC

– OTHER IMPORTANT INFORMATION –

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

Activate IDX Identity Protection Membership Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the IDX website to enroll: https://app.idx.us/account-creation/protect
3. PROVIDE the Enrollment Code found at the top of this notice.

If you have questions about the product or if you would like to enroll over the phone, please contact IDX at 1-833-764-2922.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary [redacted] 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
P.O. Box 105069
Atlanta, GA 30348
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 LLC
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.

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
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960

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'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. 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.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

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, www.oag.state.md.us/Consumer, 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.

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

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/ consumer-protection, Telephone: 202-442-9828.

* * * * *

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer

reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

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 may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

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, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

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 should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

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. You may contact these agencies using the contact information provided above.