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

October 7, 2021

VIA U.S. MAIL

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

Re: Senior Living, LLC / Pilgrim River LLC, – Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents Senior Living, LLC d/b/a Bridgeway Care and Rehab Center at Hillsborough ("Senior Living") and Pilgrim River, LLC d/b/a The Avalon Assisted Living Residence at Hillsborough ("Pilgrim River"). I am writing to provide notification of an incident at Senior Living and Pilgrim River that may affect the security of personal information of approximately two (2) New Hampshire residents. Senior Living's and Pilgrim River'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, Senior Living and Pilgrim River do not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Senior Living and Pilgrim River recently discovered unauthorized access to their network occurred between March 3, 2021 and March 7, 2021. Upon learning of the issue, Senior Living and Pilgrim River immediately took steps to secure their network and mitigate against any additional harm. Senior Living and Pilgrim River also launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and assess these types of situations to analyze the extent of any compromise of the information on the network. Based on a comprehensive investigation and document review, which concluded on September 7, 2021, Senior Living and Pilgrim River discovered that a limited amount of personal information may have been removed from the network in connection with this incident, including the affected residents' full names, Social Security numbers, medical diagnosis, and medical record number.

To date, Senior Living and Pilgrim River are not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Senior Living and Pilgrim River wanted to inform you (and the affected residents) of the incident and to explain the steps that they are taking to help safeguard the affected residents against identity fraud. Senior Living and Pilgrim River are providing the affected residents with written notification of this incident commencing on or about October 7,

2021 in substantially the same form as the letter attached hereto. Senior Living and Pilgrim River are providing 12 months of credit monitoring to any resident whose Social Security number was impacted and is advising the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Senior Living and Pilgrim River are 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 and practices and safeguards to protect against medical theft. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission

At Senior Living and Pilgrim River protecting the privacy of personal information is a top priority. Senior Living and Pilgrim River are committed to maintaining the privacy of personal information in its possession and have taken many precautions to safeguard it. Senior Living and Pilgrim River continually evaluate and modify their practices to enhance the security and privacy of the personal information they maintain.

Notice is being provided pursuant to the HIPAA Breach Notification Rule, 45 CFR §§ 164.400, *et seq.*

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.

The Avalon Bridgeway
AT HILLSBOROUGH
A Bridgeway Assisted Living Residence

[redacted]

To Enroll, Please Call:
[redacted]
Or Visit:
[redacted]
[redacted]
Enrollment Code: [redacted]

[redacted]

[redacted]

[redacted]

Dear [redacted]:

The privacy and security of the personal information we maintain is of the utmost importance to Bridgeway Care and Rehab Center at Hillsborough and The Avalon Assisted Living Residence at Hillsborough. We are writing with important information regarding a recent security incident that may have impacted your information. 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 personal information.

What Happened?

We recently discovered unauthorized access to our network occurred between March 3, 2021 and March 7, 2021. Upon learning of the issue, we immediately took steps to secure our network and mitigate against any additional harm.

What We Are Doing

We launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze these types of situations 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 September 7, 2021 that documents containing your personal and/or protected health information were acquired from our network as a result of the incident.

What Information Was Involved?

Based on our extensive manual review and analysis of the data at issue, we determined that certain data removed from our network contained your [redacted].

What You Can Do

To date, we are not aware of any reports of identity fraud or improper use of your personal information as a direct result of this incident. Out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary one-year membership of identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 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.

This letter also provides other 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. To the extent it is helpful, we have also provided information on protecting 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 protect against misuse of your information. The response line is available Monday through Friday, **9am to 9pm Eastern** time.

Sincerely,

Bridgeway Care and Rehab Center at Hillsborough
and
The Avalon Assisted Living Residence at Hillsborough

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-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: [redacted]
3. PROVIDE the [redacted]: Found above in this letter

If you have questions about the product or if you would like to enroll over the phone, please contact IDX at [redacted].

2. 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-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 105788
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 6790
Fullerton, PA 92834-6790
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
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 2000
Chester, PA 19016
http://www.transunion.com/security 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 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.

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, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

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.

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;
8. If you are not a victim of identity theft, payment. Do not send cash through the mail.

There were two Rhode Island residents impacted by this incident.

6. Protecting Your Medical Information.

If this notice letter indicates that your medical information was impacted, we have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from 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.