McDonald Hopkins
A business advisory and advocacy law firm®

100 International Drive
23rd Floor
Baltimore, MD 21202

P 1.248.646.5070
F 1.248.646.5075

**Spencer S. Pollock, CIPP/US, CIPM**
Direct Dial: (410) 456-2741
Cell: (410) 917-5189
E-mail: spollock@mcdonaldhopkins.com

RECEIVED
JUL 11 2022
CONSUMER PROTECTION

July 5, 2022

**Privileged and Confidential**
**VIA CERTIFIED FIRST-CLASS MAIL**
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

**Re: Security Breach Notification**

To Whom It May Concern,

We are writing on behalf of our client, Sherrill House, Inc. ("Sherrill House") (located at 135 S. Huntington Ave., Boston, MA 02130) to notify you of a data security incident involving forty-three (43) New Hampshire residents.[1]

**Nature**

On November 4, 2021, Sherrill House discovered suspicious activity in one of its employee email accounts involving an attempt to fraudulently transfer funds. At that time, Sherrill House's technology team acted quickly to secure its systems through a variety of methods. Sherrill House also engaged third-party independent cybersecurity experts to conduct an investigation into the incident.

At the conclusion of the investigation, Sherrill House determined that an unauthorized individual or individuals gained access to three email accounts on or around September 4, 2021. At that time, Sherrill House began a comprehensive review of the affected email accounts and determined that the impacted data contained protected personal and health information. Concurrently, Sherrill House provided substitute notice on its website. With this said, as of now, Sherrill House has no evidence indicating that any information has been used for identity theft or financial fraud.

Sherrill House recently completed its review to identify the individuals who had personal information or protected health information impacted by the incident. On June 29, 2022, Sherrill House concluded its review and located the most recent contact information for these individuals. Sherrill House determined that the incident potentially involved forty-three (43) New Hampshire residents.

The personal information obtained potentially included demographic information (first and last name, gender, home address, phone number, and date of birth); driver's license numbers; state identification card

[1] By providing this notice, Sherrill House does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

numbers; usernames and passwords; Social Security Numbers; financial account information; clinical information (medical history/diagnosis/treatment, dates of service, lab test results, prescription information, provider name, medical account number, or anything similar in the medical file and/or record); and health insurance information (policy and claim information).

**Notice and Sherrill House's Response to the Event**

On July 5, 2022, Sherrill House will mail a written notification to the potentially affected New Hampshire residents, pursuant to N.H. Rev. State § 359-C:19, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, Sherrill House is providing the potentially impacted individuals the following:

- Free access to credit monitoring services for two years through TransUnion;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Further, Sherrill House provided notice to the applicable government regulators, officials, and other state Attorneys General (as necessary). Finally, Sherrill House is working to implement any necessary additional safeguards; enhance and improve its policies and procedures related to data protection; improve its cybersecurity infrastructure; and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

**Contact Information**

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 456-2741 or email me at spollock@mcdonaldhopkins.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

# EXHIBIT A

Sherrill House, Inc
P.O. Box 3923
Syracuse, NY 13220

Sherrill House
A Not-for-profit Skilled Nursing & Rehabilitation Center
135 S. Huntington Ave.
Boston, MA 02130

[redacted]

July 5, 2022

Re: Notice of Data Breach

Dear [redacted]

At Sherrill House, we value transparency and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your protected personal information, what we did in response, and steps you can take to protect yourself against possible misuse of the information.

**What Happened**
On November 4, 2021, we discovered suspicious activity in one of our employee email accounts involving an attempt to fraudulently transfer funds. At that time, our technology team acted quickly to secure our systems through a variety of methods. We also engaged third-party independent cybersecurity experts to conduct an investigation into the incident.

At the conclusion of the investigation, we determined that an unauthorized individual or individuals gained access to three of our email accounts on or around September 4, 2021 and as a result, potentially obtained protected personal information. At that time, we also began a comprehensive review of the affected email accounts and determined that the impacted data may have contained some of your protected personal information. Based on our investigation, and the nature of the fraudulent activity, we believe this was solely an attempt to obtain funds from our financial account (which was not successful), and have no evidence that your information has been used for identity theft or financial fraud. However, we wanted to notify you of the incident out of an abundance of caution and provide you information on how to best protect your identity.

**What Information Was Involved**
The types of information included your [redacted]

***To reiterate, we have no evidence indicating that any information has been used for identity theft or financial fraud.***

**What We Are Doing**
The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, we are implementing additional cybersecurity safeguards, as needed, enhancing our employee cybersecurity training, and improving our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

**What You Can Do**

As stated above, while we have no evidence indicating that your information has been used for identity theft or fraud, we strongly recommend that you remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity to the institution that issued the record, as well as law enforcement. In addition, please see "***OTHER IMPORTANT INFORMATION***" on the following pages for guidance on how to best protect your identity.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

Finally, we are providing you with access to Single Bureau Credit Monitoring* services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

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]

**For More Information**

We sincerely regret this incident occurred and for any concern it may cause. We understand that you may have questions about what happened beyond what is covered in this letter. If you have additional questions, please call the dedicated toll-free helpline set up specifically for this purpose at [redacted] Eastern time, excluding major U.S. holidays).

Sincerely,

Adam J. Fumia
Chief Information Officer

* Services marked with an "*" require 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.

## OTHER IMPORTANT INFORMATION

**Obtain and Monitor Your Credit Report.** We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/index.action. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

| Equifax | Experian | TransUnion |
|---|---|---|
| **(888) 766-0008** | (888) 397-3742 | (800) 680-7289 |
| P.O. Box 740256 | P.O. Box 2104 | P.O. Box 1000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19016 |
| www.equifax.com | www.experian.com | www.transunion.com |

**Security Freeze (also known as a Credit Freeze).** Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. In addition, in some states, the agency cannot charge you to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below).

| Equifax Security Freeze | Experian Security Freeze | TransUnion |
|---|---|---|
| P.O. Box 105788 | P.O. Box 9554 | **Security Freeze & Fraud Victim Assistance Dept.** |
| Atlanta, GA 30348 | Allen, TX 75013 | P.O. Box 380 |
| https://www.equifax.com/personal/credit-report-services/credit-freeze/ | www.experian.com/freeze | Woodlyn, PA 19094 |
| | | https://www.transunion.com/credit-freeze |

**Consider Placing a Fraud Alert on Your Credit Report.** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

**Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity.** As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

**Take Advantage of Additional Free Resources on Identity Theft.** We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit

IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/.

**District of Columbia residents**: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov. **Iowa residents** may also wish to contact the Office of the Attorney general on how to avoid identity theft by calling 515-281-5164 or by mailing a letter to the Attorney General at: *Office of the Attorney General of Iowa,* Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319. **Maryland residents** may wish to review the information the Attorney General, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us. **Massachusetts residents**: State law advises you that you have the right to obtain a police report. Further, you have the right to obtain a security freeze on your credit report free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. To request a security freeze be placed on your credit report, please be prepared to provide any or all of the following: your full name, social security number, address(es), date of birth, a copy of a government issued identification card, a copy of a utility bill, bank or insurance information, or anything else the credit reporting agency needs to place the security freeze. Further information regarding credit freezes, including the contact information for the credit reporting agencies, may be found above in section titled "Security Freeze (also known as a Credit Freeze)." **New Hampshire residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above. **New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit. **New York Residents**: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: New York Attorney General's Office Bureau of Internet and Technology, (212) 416-8433, https://ag.ny.gov/internet/resource-center and or NYS Department of State's Division of Consumer Protection, (800) 697-1220, https://www.dos.ny.gov/consumerprotection. **North Carolina residents** may wish to review the information provided by the North Carolina Attorney General at www.ncdoj.gov, or by contacting the Attorney General by calling 877-5-NO-SCAM (Toll-free within North Carolina) or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office, Consumer Protection Division,* 9001 Mail Service Center Raleigh, NC 27699. **Oregon Residents**: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877- 9392, www.doj.state.or.us. **Rhode Island residents** have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. **West Virginia residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above.