

September 7, 2023

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Dear Sir or Madam:

On behalf of Ryders Health Management LLC and its affiliated entities (collectively, “Ryders”), and pursuant to the Personal Information Protection Act (“PIPA”), Md. CodeAnn. Comm. Law 14-3504, this letter provides notice of a recent data security incident. By providing this notice, Ryders does not waive any rights or defenses regarding the applicability of Maryland law, including the applicability of the Maryland data notification laws or personal jurisdiction.

Ryders manages assisted living facilities and is an entity covered by the Health Insurance Portability and Accountability Act (“HIPAA”) and is providing notification, as well as taking other steps, as required by and in compliance with HIPAA.

On July 9, 2023, Ryders detected unauthorized activity on its network, including the deployment of an encryption process and other indicators consistent with a ransomware incident. Ryders responded immediately, including by proactively taking certain systems offline, changing passwords, and launching an investigation. Ryders notified federal law enforcement of the incident and will continue to cooperate with their investigation into the party responsible. Ryders has also engaged data privacy and security professionals to conduct a forensic investigation and determine the incident’s scope. The Ryders investigation determined that for a brief amount of time in July, an unauthorized actor obtained access to systems and downloaded data, seemingly for the sole purpose of demanding a ransom. Ryders then immediately began analyzing the records involved to confirm the identities of those potentially affected and notify them. There is currently no evidence that any information has been misused for identity theft or fraud in connection with the incident.

Upon becoming aware of the incident, Ryders immediately implemented measures to further improve the security of their systems and practices. Ryders worked with leading data privacy and security professionals to aid in their response and have reported this incident to relevant government agencies and federal law enforcement. Ryders also implemented additional security protocols designed to protect their network, email environment, and systems, and are currently assessing the entirety of their information security program.

Pursuant to HIPAA, Ryders has timely notified the Department of Health and Human Resource’s

Office of the Attorney General

September 7, 2023

Page 2

Office for Civil Rights, as well as provided direct notice to the affected individuals. Ryders has identified that the incident involved the personal health information of three (3) Maryland residents. While the data elements varied by individual, the elements included were: name, address, date of birth, Social Security number, date(s) of service, medical record number and identification numbers, care plan, provider and facility name, medications and lab results, diagnostic and treatment information, health insurance information, and healthcare payment information. Attached for your convenience is a copy of the template notification that was sent via regular mail to the impacted residents on September 7, 2023, which also includes an offer for twenty-four (24) months of cost-free credit monitoring.

Please feel free to contact me with any questions at (716) 898-2102 or dgreene@octillolaw.com.

Sincerely,

OCTILLO

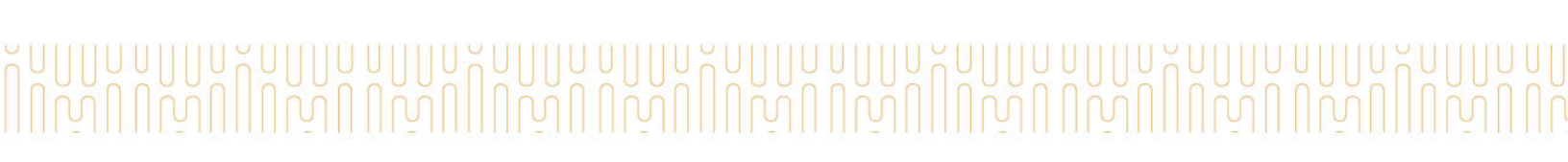
A handwritten signature in black ink, appearing to read 'D. Greene', with a stylized flourish extending to the right.

Daniel P. Greene, Esq.

Certified Information Privacy Professional, United States (CIPP/US)

Certified Information Privacy Professional, Europe (CIPP/E)

Encl.





Ryders Health Management

Return Mail Processing
PO Box 999
Suwanee, GA 30024

GOVERNING BOARD
Martin Sbriglio, RN, NHA, CEO
Dr. Robert Sbriglio, MD, MPH,
Chief Medical Officer



25 1 7243 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



- ☐ Aaron Manor Nursing & Rehabilitation Center
- ☐ Lord Chamberlain Nursing & Rehabilitation Center
- ☐ Bel-Air Manor Nursing & Rehabilitation Center
- ☐ Mystic Healthcare & Rehabilitation Center
- ☐ Cheshire House Nursing & Rehabilitation Center
- ☐ Lighthouse Companion Care
- ☐ Douglas Manor Nursing & Rehabilitation Center
- ☐ Lighthouse Home Health Care
- ☐ Greentree Manor Nursing & Rehabilitation Center
- ☐ Ryders Rehabilitation
- ☐ Lord Chamberlain Manor Nursing & Rehabilitation Center
- ☐ Ryders Health Management

September 7, 2023

Dear Sample A. Sample:

Ryders Health Management provides skilled nursing and rehabilitation services at the following facilities: Lord Chamberlain Manor Nursing & Rehabilitation Center, Lord Chamberlain Nursing & Rehabilitation Center, Douglas Manor Nursing & Rehabilitation Center, Greentree Manor Nursing & Rehabilitation Center, Mystic Healthcare & Rehabilitation Center. I am writing to inform you that we, Ryders Health Management (“Ryders” or “we”) recently experienced a data incident (“Incident”) which potentially involved your personal information (“Information”) given you or a loved one received services at one of the listed locations. This letter provides you with information about this Incident, our response, steps you can take, and if necessary, information on where to direct your questions. Additionally, although we are unaware of any misuse of your Information or fraud in relation to the Incident, as a precaution we have also provided steps you can take to protect your Information.

What Happened?

On July 9, 2023, we detected unauthorized activity in our network, including the deployment of an encryption process and other indicators consistent with a ransomware incident. Ryders responded immediately, including by proactively taking certain systems offline, changing passwords, and launching an investigation. Ryders notified federal law enforcement of the incident and will continue to cooperate with their investigation into the party responsible. Our investigation determined that for a brief amount of time in July, an unauthorized actor obtained access to our systems and downloaded data, seemingly for the sole purpose of demanding a ransom. We then immediately began analyzing the records involved to confirm the identities of those potentially affected and notify them. There is currently no evidence that any Information has been misused for identity theft or fraud in connection with the Incident.

What Information Was Involved?

We determined that the following types of Information may have been impacted: name, address, date of birth, Social Security number, date(s) of service, medical record number and identification numbers, care plan, provider and facility name, medications and lab results, diagnostic and treatment information, health insurance information, and healthcare payment information. Note that this describes general categories of Information involved in this Incident, and it likely includes categories that are not relevant to you. If you would like to learn more about the specific types of Information related to you that were impacted, please call 833-549-2142 to inquire.

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further improve the security of our systems and practices. We worked with leading data privacy and security professionals to aid in our response and have reported this Incident to relevant government agencies and federal law enforcement. We also implemented additional security protocols designed to protect our network, email environment, and systems, and are currently assessing the entirety of our information security program.

What Can You Do?

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twenty-four (24) months.

Please note that Identity Restoration is available to you for twenty-four (24) months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twenty-four (24) month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- **Enroll by** December 31, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: **ABCDEFGHI**

While credit monitoring services are available to you at no cost for twenty-four (24) months, it is always recommended that you remain vigilant, regularly monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Please also review the “Additional Resources” section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have further questions or concerns, would like more insight into the data about you that was potentially impacted, or would like an alternative to enrolling online, please call 833-549-2142 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Please be prepared to provide your engagement number B103248 as proof of eligibility for the Identity Restoration services by Experian.

Sincerely,



Martin Sbriglio
Chief Executive Officer

Encl.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also 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, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. 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 place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

For New Mexico Residents: 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.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Alabama Residents: You may contact the Attorney General's Office for the State of Alabama, Consumer Protection Division, 501 Washington Avenue, Montgomery, AL 36104, www.oag.state.md.us, 1-800-392-5658.

For District of Columbia Residents: You may contact the District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, (202) 442-9828.

For Illinois Residents: You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800-964-3013.

For Iowa Residents: You may contact the Iowa Office of the Attorney General, 1305 E. Walnut Street, Des Moines IA 50319, consumer@ag.iowa.gov, 1-888-777-4590.

For Kansas Residents: You may contact the Kansas Office of the Attorney General, Consumer Protection Division, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, <https://ag.ks.gov/>, 1-800-432-2310.

For Kentucky Residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For Minnesota Residents: You may contact the Minnesota Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392-8222.

For New Mexico Residents: You may contact the New Mexico Office of the Attorney General, Consumer Protection Division, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501, www.nmag.gov, 1-844-255-9210.

For New York Residents: You may contact the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <https://ag.ny.gov>, 1-800-771-7755.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa Residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts Residents: You have the right to obtain a police report if you are a victim of identity theft.

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island Residents: Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.