



Sean B. Hoar
888 SW Fifth Avenue Ste. 900
Portland, OR 97204
Sean.Hoar@lewisbrisbois.com
Direct: 971.712.2795

July 16, 2020

VIA E-MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
E-Mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Lorien Health Services, (“Lorien”) a Maryland-based company that provides assisted living and skilled nursing interventions for seniors across ten facilities, in connection with a data security incident which is described in greater detail below. This letter is being sent pursuant to N.H. Rev. Stat. §§ 359-C:19 - C:21 because the personal information of New Hampshire residents may have been affected by a recent data security incident. The incident may have involved unauthorized access to names, addresses, Social Security numbers, dates of birth, and health diagnosis and treatment information of residents and employees of Lorien.

On June 6, 2020, Lorien learned that data on its network had been encrypted. Upon discovering this incident, Lorien immediately engaged a team of cybersecurity experts to assist with its response and to determine whether any personal information may have been accessed during the incident. On June 10, 2020 the investigation determined that personal information may have been accessed during the incident. Lorien then worked to identify potentially affected persons. On July 9, 2020, Lorien identified three (3) New Hampshire residents as among the potentially affected population. Lorien has reported this incident to law enforcement.

In addition to restoring its system, Lorien has implemented enhanced security measures to minimize the likelihood that an event like this might occur again in the future. Lorien notified the potentially affected New Hampshire residents via the attached sample letter on July 16, 2020. Out of an abundance of caution, Lorien is offering twelve (12) months of complimentary credit and identity monitoring services to the potentially affected residents through ID Experts.

July 16, 2020
Page 2

Please contact me should you have any questions.

Sincerely,



Sean B. Hoar of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Consumer Notification Letter



C/O ID Experts
PO Box 4600
Everett WA 98204

ENDORSE



<<First Name>> <<Last Name>>



ADDRESS1
ADDRESS2
CSZ
COUNTRY

SEQ
CODE 2D
Ver ADU

BREAK

To Enroll, Please Call:
1-833-431-1278
Or Visit:
<https://app.myidcare.com/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

July 16, 2020

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident that involved your personal information. At Lorien Health Services (“Lorien”), which you may know as FACILITY, we take the privacy and security of your information very seriously. This is why I am notifying you of the incident, offering you credit monitoring and identity monitoring services, and informing you about steps you can take to help protect your personal information.

What Happened? On June 6, 2020, Lorien learned that data on our network had been encrypted. Upon discovering this incident, Lorien immediately engaged a team of cybersecurity experts to assist with our response and to determine whether any personal information may have been accessed during the incident. On June 10, 2020 the investigation determined that your information may have been accessed during the incident.

What Information Was Involved? The information involved resident admission forms which typically include names, Social Security numbers, dates of birth, addresses, and health diagnosis and treatment information.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators accountable. In addition, we are providing you with information to help protect your personal information, and offering identity monitoring and recovery services for 12 months through IDExperts as described below.

What You Can Do: You can follow the recommendations included with this letter to protect your personal information. We strongly encourage you to enroll in the credit monitoring and identity protection services through ID Experts. To enroll, please visit <https://app.myidcare.com/account-creation/protect> or 1-833-431-1278 and provide the following enrollment code: <<XXXXXXXXXX>>. Please note you must enroll by October 16, 2020. If you have questions or need assistance, please call ID Experts at 1-833-431-1278.

For More Information: If you have any questions about this letter, please contact Lorien at 1-833-431-1278. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Lou Grimmel, Sr.
Chief Executive Officer, Lorien Health Services

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major 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 print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 annualcreditreport.com
---	---	--	---

Fraud Alert: 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 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland can obtain more information from their Attorney General using the contact information below.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov , and www.ftc.gov/idtheft 1-877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400
---	---	---	--

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/documents/bcftp_consumer-rights-summary_2018-09.docx.