LEWIS BRISBOIS
LEWIS BRISBOIS BISGAARD & SMITH LLP

Shelly Hall
550 West Adams Street Suite 300
Chicago, IL 60661
Shelly.Hall@lewisbrisbois.com
Direct: 312.463.3362

November 23, 2021

VIA EMAIL
Attorney General Gordon J. MacDonald
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

Lewis Brisbois Bisgaard & Smith LLP represents MRI Network ("MRI"), a franchisor headquartered in Fort Lauderdale, Florida, in connection with a recent data security incident that may have affected the information of certain New Hampshire residents.

1. NATURE OF THE SECURITY INCIDENT

On July 30, 2021, MRI learned of a security incident involving unauthorized access to an employee's email account. Upon discovering the unauthorized access, MRI's information technology team and cybersecurity experts immediately began an investigation to address the incident. Through this investigation, MRI determined that an unauthorized party accessed one employee's email account from July 8 to July 30, 2021.

MRI undertook a review of the information that could have potentially been accessed as a result of the incident, and, on October 29, 2021, determined that the information related to its customers and employees, including the personal information of seven (7) New Hampshire residents. The information accessed without authorization included the first and last name, address, date of birth, financial account information, medical information and/or Social Security number. To date, MRI has no evidence that any of this information has been misused.

2. NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

MRI started notifying the seven (7) New Hampshire residents of this data security incident via first class U.S. mail on November 23, 2021. A sample copy of the notification letter sent to the affected individuals is attached.

3. STEPS TAKEN RELATING TO THE INCIDENT

To help prevent something like this from happening again, MRI is implementing additional technical security measures and increasing employee cybersecurity training. While MRI has no indication that the information has been misused, it nonetheless is providing individuals with information about steps that they can take to help protect their personal information. As a further precaution, MRI is also offering consumers one year of complimentary credit and identity monitoring services through IDX. This product helps detect possible misuse of personal information and provides consumers whose information may have been accessed without authorization with identity protection support. Furthermore, MRI provided affected consumers with information about steps that they can take protect their personal information.

4. CONTACT INFORMATION

Please feel free to contact me at (312) 463.3362 or Shelly.Hall@lewisbrisbois.com if you have any further questions.

Respectfully,

Shelly Hall of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Individual Notification Letter

MRI Network
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

November 23, 2021

Subject: Notice of Data Security Incident

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

At MRI Network ("MRI") we are committed to protecting the confidentiality and security of the information we receive and maintain. We are writing to inform you of a recent data security incident we experienced that may have involved some of your information. While we are unaware of any misuse of your information, we are notifying you of the incident and informing you about steps you can take to help protect it.

What Happened: On July 30, 2021, we learned of a security incident involving unauthorized access to an employee's email account. Upon discovering the unauthorized access, our information technology team and cybersecurity experts began an investigation to determine what happened and to address the incident.

What Information Was Involved: We completed a comprehensive review of the data that could have potentially been affected by the unauthorized access from July 8 to July 30, 2021. We completed that review on October 29, 2021 and determined that your information may have been impacted by this incident, including name, address, date of birth, financial account information, medical information and/or Social Security numbers.

What We Are Doing: To help prevent something like this from happening again, we implemented additional technical security measures and employee cybersecurity training. While we have no indication that your information has been misused, we are nonetheless providing you with information about steps that you can take to help protect your personal information. As a further precaution, we are also offering you <<months>> of complimentary credit and identity monitoring services through IDX. This product helps detect possible misuse of your information and provides you with identity protection support.

What You Can Do: You can enroll in IDX's complimentary credit and identity monitoring services by going to https://app.idx.us/account-creation/protect or calling 1-800-939-4170. When prompted, please provide the unique code at the top of this letter to enroll in the services. The deadline to enroll is February 23, 2022. For more information on how you can protect your personal information, please review the resources provided on the following pages.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-800-939-4170 between 6am to 6pm Pacific Time Monday through Friday.

The security of your information is a top priority for MRI. We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

MRI Network

ADDITIONAL 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts and Credit or Security Freezes:

***Fraud Alerts*:** There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. 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.

Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

***Credit or Security Freeze*s:** Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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.

How do I place a freeze on my credit reports? You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact each of the credit reporting agencies identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

How do I lift a freeze from my credit reports? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.

MRI can be reached via mail at: 2400 East Commercial Boulevard Suite 718, Fort Lauderdale, FL 33308, and via phone: 800.875.4000

Additional information for residents of the following states:

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202, 1-888-743-0023, oag.state.md.us. MRI can be reached via mail at: 2400 East Commercial Boulevard Suite 718, Fort Lauderdale, FL 33308, and via phone: 800.875.4000.

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005, 1-212-416-8433, https://ag.ny.gov/.

Rhode Island: 1 Rhode Island resident may have been affected by the Incident. Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov.

Washington D.C.: Washington D.C. Attorney General can be reached at: 441 4th Street, NW Washington, DC 20001, 1-202-727-3400, oag.dc.gov.