LEWIS BRISBOIS BISGAARD & SMITH LLP

Maria Efaplomatidis
77 Water Street, Suite 2100
New York, NY 10005
Maria.Efaplomatidis@lewisbrisbois.com
Direct: 212.232.1366

October 8, 2021

VIA E-MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

Lewis Brisbois Bisgaard & Smith LLP represents EMJ Corporation ("EMJ") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification statute.

1. Nature of the Security Incident

EMJ is a group of construction services companies, based in Chattanooga, Tennessee.

On September 5, 2021, EMJ experienced a network disruption and upon investigation, it discovered an encryption incident and immediately took immediate steps to secure the environment. EMJ also launched an investigation and engaged a digital forensics firm to determine what happened and what information may have been accessed.

The investigation revealed that an unauthorized actor leveraged an EMJ admin account to access and exfiltrate data out of the environment. Based on the findings from the investigation, EMJ reviewed a list of locations and the compressed archive which contains the data exfiltrated, and determined that it contained personal information. EMJ then worked diligently to identify addresses for the individuals whose information may have been involved. EMJ completed that process on September 24, 2021.

2. Type of Information and Number of New Hampshire Residents Involved

The incident involved personal information for 13 New Hampshire residents. The information involved for the residents may have included Form W-2, Wage and Tax Statement, which could have included Social Security numbers.

The affected individuals will receive a letter notifying them of the incident, offering complimentary identity monitoring services for 24 months, and providing additional steps they can take to protect their personal information. The notification letters were sent via USPS First Class Mail on September 27, 2021.

3. Measures Taken to Address the Incident

In response to the incident, EMJ retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise.

Additionally, as discussed above, EMJ is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in the complimentary identity monitoring services offered in the notification letter.

4. Contact Information

EMJ is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Maria Efaplomatidis at 212.232.1366 or Maria.Efaplomatidis@lewisbrisbois.com.

Sincerely,

Maria Efaplomatidis of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Consumer Notification Letter

EMJ CORPORATION

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Subject: Notice of Data Incident

Dear <<Name1>>:

I am writing to inform you of a data security incident that may have affected your personal information. EMJ Corporation and its affiliates ("EMJ"), takes the privacy and security of personal information very seriously. This is why we are informing you about the incident and steps you can take to protect your information, and offering you complimentary identity protection services.

What Happened: On September 5, 2021, we experienced a network disruption. We immediately initiated an investigation and engaged cybersecurity experts to assist us with the process. Our investigation determined that personal information was affected. We have learned that your information may have been accessed without authorization.

What Information Was Involved: The information may have involved your Form W-2, Wage and Tax Statement, which would include your Social Security number.

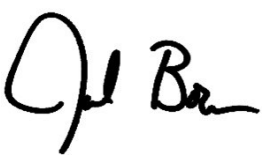
What We Are Doing: In addition to the items noted above, we are taking the following measures:

- Working with the FBI and will provide whatever cooperation is necessary to hold the perpetrators accountable.
- Enhancing the security of our network to reduce the risk of a similar incident occurring in the future.
- Providing former and current employees information about how to protect personal information.
- Offering former and current employees free credit monitoring and identity theft restoration services through TransUnion Interactive, asubsidiary of TransUnion®, one of the three nationwide credit reporting companies. Your identity monitoring services include credit monitoring, a $1 million identity fraud loss reimbursement policy, and identity theft restoration.

What You Can Do: You can follow the recommendations on the following page to protect your personal information. We encourage you to enroll in the credit monitoring and identity monitoring services to protect your personal information. To enroll, please visit www.mytrueidentity.com or call 1-855-288-5422 and provide the following enrollment code: <<Activation Code>> along with the 6-digit Telephone Pass Code <<Pass Code>>. Please note you must enroll by <<Enrollment Deadline>>. If you have questions or need assistance enrolling, please call 1-855-288-5422.

For More Information: If you have questions about this letter, please contact our dedicated call center at 1-800-974-6541, Monday through Friday, 9:00 a.m. to 9:00 p.m., Eastern Time. We sincerely apologize for this issue and are working to resolve it quickly, and with as minimal impact as possible.

Sincerely,



Jack Bowen, President and CEO
EMJ Corporation

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for twenty-four months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code <<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code <<Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain twenty-four months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.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 one year. 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: 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.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

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

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 other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.