FOLEY
FOLEY & LARDNER LLP

ATTORNEYS AT LAW
777 EAST WISCONSIN AVENUE
MILWAUKEE, WI 53202-5306
414.271.2400 TEL
414.297.4900 FAX
WWW.FOLEY.COM

jrathburn@foley.com
414.297.5864

CLIENT/MATTER NUMBER
105349-0224

September 29, 2020

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification Pursuant to N.H. Rev. Stat. § 359-C:19 *et seq.*

Dear Attorney General MacDonald:

We are writing on behalf of our client, Jani-King International, Inc. ("JKI"), to notify you of a breach of security involving one (1) New Hampshire resident.

NATURE OF THE UNAUTHORIZED DISCLOSURE

JKI experienced a phishing attack on JKI's email system that potentially compromised sensitive employee information on June 5, 2020. JKI became aware of this incident on July 31, 2020 and took immediate steps to both contain and thoroughly investigate the attack. Although JKI has no evidence to suggest that any information was actually accessed, viewed, or otherwise acquired by the unauthorized third party, it notified individuals out of an abundance of caution because this incident, by its nature, could have allowed such third party to access, use, and/or disclose individuals' full names, addresses, dates of birth, Social Security numbers, driver's license numbers, and bank account information.

STEPS WE ARE TAKING RELATED TO THE INCIDENT

JKI mailed a notification to the potentially affected New Hampshire resident on September 29, 2020. Enclosed is a sample copy of the notice that was sent to that individual.

Out of an abundance of caution, JKI provided the potentially affected New Hampshire resident with credit monitoring and identity protection services through TransUnion Interactive, a subsidiary of TransUnion®, at no charge for a period of twenty-four (24) months, and has also set up a dedicated support line that will be staffed to answer any questions individuals may have about this incident or the services available to them.

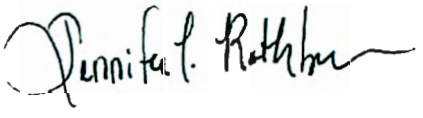
In response to this incident, JKI implemented additional security measures to help protect the privacy of individuals' information that it maintains, including establishing a new clean network with fresh operating systems installed. JKI also hired forensic consultants to remediate the incident, block malicious software and deploy an endpoint security solution across all of its systems to detect any further malicious activity.

FOLEY

FOLEY & LARDNER LLP

If you have any further inquiries concerning this notification, please do not hesitate to contact me.

Sincerely,



Jennifer L. Rathburn

Encl: Sample Notification Letter

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>>
<<Address 5>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

WHAT HAPPENED?

At Jani-King International, Inc. and its affiliated companies (collectively referred to as "JKI"), we value and respect the privacy of your information, which is why, as a precautionary measure, we are writing to inform you of a phishing attack on JKI's email system that potentially compromised sensitive employee information on June 5, 2020. We became aware of this incident on July 31, 2020 and took immediate steps to both contain and thoroughly investigate this attack. Although we have no evidence to suggest that any information was actually accessed, viewed, or otherwise acquired by the unauthorized third party, we are notifying you out of an abundance of caution because this incident, by its nature, could have allowed such third party to access, use, and/or disclose your information.

WHAT INFORMATION WAS INVOLVED?

The type of sensitive information that potentially could have been involved in the phishing attack includes your full name, address, date of birth, Social Security number, driver's license number, and bank account information.

WHAT WE ARE DOING

In response to this incident, we implemented additional security measures to help protect the privacy of your information, including establishing a new clean network with fresh operating systems installed. We also hired forensic consultants to remediate the incident, block malicious software and deploy an endpoint security solution across all of our systems to detect any further malicious activity.

To help relieve concerns and restore confidence following this incident, we have arranged for you to enroll, at no cost to you, in a comprehensive credit monitoring and identity restoration service (*my*TrueIdentity) for two (2) years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. These services help detect possible misuse of your personal information and provide you with identity protection services focused on immediate identification and resolution. These services are completely free and will not impact your credit score. You may sign up for these services online or via U.S. mail delivery by following the instructions attached to this notice.

WHAT YOU CAN DO

Please review the enclosed "Other Important Information" document included with this letter for further steps you can take to protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. It is also recommended that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit reports for unauthorized activity. If you discover any suspicious or unusual activity on your accounts, you should promptly notify the financial institution or company with which your account is maintained.

FOR MORE INFORMATION

For further information and assistance, please our dedicated incident response line at 888-490-0890 between 8 a.m. – 8 p.m. Central Time, Monday through Friday.

Sincerely,

Jerry Crawford
President & CEO
Jani-King International, Inc.

OTHER IMPORTANT INFORMATION

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 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 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.

Fraud Alert. You have the right to place an initial or extended "fraud alert" on your file at no cost by contacting any of the three nationwide credit reporting agencies identified above. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert, which lasts for 7 years, on your credit file.

Security Freeze. You have the right to place, lift, or remove a "security freeze" on your credit report, free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. 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, display your name and current mailing address, and the date of issue. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or up to 3 business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the 3 credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to remove the security freeze.

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 FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (438-4338).

- **For California Residents**: You may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.
- **For District of Columbia Residents**: You may obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia by visiting https://oag.dc.gov/consumer-protection, emailing consumer.protection@dc.gov, calling (202) 442-9828, or mailing Office of the Attorney General, Office of Consumer Protection 400 6th Street, NW Washington, DC 20001.
- **For Iowa Residents**: You are advised to report suspected incidents of identity theft to law enforcement or the Iowa Attorney General's Office at Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 1-515-281-5926 or 1-888-777-4590.
- **For Maryland Residents**: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, Telephone: 1-410-576-6491 or 1-888-743-0023.
- **For New Mexico residents**: You have rights pursuant to the Fair Credit Reporting Act ("FCRA"), 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 FCRA, 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 reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response 30-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.
- **For North Carolina Residents**: You may obtain additional information about preventing identity theft provided by the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/identity-theft/, by calling 1-877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.
- **For New York Residents**: You may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General at https://ag.ny.gov/ or by calling 1-800-771-7755; the New York State Police at http://troopers.ny.gov/ or by calling 1-518-457-6721; and/or the New York Department of State at https://www.dos.ny.gov or by calling 1-800-697-1220.

Enroll in Credit Monitoring/Identity Restoration Services. As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 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 six-digit telephone passcode **<<Enagagement Number>>** 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.

You can sign up for the online or offline 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 a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. 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, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)