May 3, 2023

VIA OVERNIGHT MAIL

Office of the Attorney General of New Hampshire
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

I write on behalf of Richards Industrials, Inc. ("Richards"), a leading manufacturer of pressure regulators, control valves, instrument hand valves and steam traps, with respect to a data security event involving certain personal information of New Hampshire residents. By providing this notice, Richards does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On February 5, 2023, Richards learned that an unauthorized actor had obtained access to Richards's network and was beginning to encrypt it. Richards swiftly disconnected its network from the Internet, and began investigating the incident with the assistance of an independent forensic provider. That forensic investigation determined that the unauthorized actor had access to Richards' network for just over three hours on February 5, 2023. During that time, the unauthorized user repeatedly attempted to remove files from Richard's systems, but Richards has no conclusive indication that the unauthorized user was successful in doing so. Nonetheless, out of an abundance of caution, Richards is providing you – and affected individuals – with notice of this incident.

While Richards discovered the incident on February 5, 2023, before Richards could access its network, it had to be restored from a backup. That process lasted until mid-February. At that point, Richards began the processing of collecting the information that the threat actor attempted to export, and begin a manual review of the data to identify potentially impacted individuals. That process concluded on April 18, 2023. Richards then had to locate addresses for the impacted persons, which process completed on April 26, 2023. Only then was Richards able to confirm that there was approximately one New Hampshire resident affected by this incident.

The affected information varied from individual to individual, but generally included ,

. Richards will be providing notice of this incident and credit monitoring to the one New Hampshire resident affected by this incident.

McDermott
Will & Emery

444 West Lake Street Chicago IL 60606-0029 Tel +1 312 372 2000 Fax +1 312 984 7700
US practice conducted through McDermott Will & Emery LLP.

During its investigation, Richards promptly contained the incident and blocked the unauthorized party from accessing the Richards network. Richards worked with a third party forensic provider to confirm that the unauthorized third party no longer had access to Richards's network. Richards has taken steps to enhance its data security measures to prevent the occurrence of a similar event in the future, including forced password resets, changes to Richards's firewall configuration, and additional detection safeguards to its corporate network.

Richards will send notification letters to the affected New Hampshire resident on May 4, 2023 via regular U.S. mail. A copy of the template notification letter is enclosed. In addition, Richards is offering complimentary credit monitoring and identity protection services through Kroll to the affected individual for 24 months.

If you have any questions, please contact me at .

Sincerely,

David Saunders

Enclosures

RICHARDS
INDUSTRIALS

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

RE: *Notice of Data Breach*

Dear <<first_name>>:

Richards Industrials, Inc. ("Richards") is writing to inform you of an incident that involved your personal information. We are reaching out to explain the circumstances of the incident, the types of information involved, what we are doing and have done in response to the event, and steps that can be taken to help protect your information. Please read this letter carefully.

What happened? In February 2023, Richards learned that an unauthorized individual had obtained access to our corporate network. Our team immediately began investigating this incident with the assistance of forensic providers. Based on our investigation, an unauthorized user gained access to Richards' corporate network, and attempted to remove certain files, including files which contained personal information. We have no conclusive evidence that the attempt to remove files was successful. However, out of an abundance of caution, we wanted to notify you of this incident since your personal information was in one or more of the files that the unauthorized user attempted to remove from Richards' systems.

What information was involved? The affected information varied for each individual based on the files that were on our network. However, the files may have included your first and last name, health insurance information, health information, account access credentials, address, passport, U.S. Alien Registration Number, tax ID, driver's license or Social Security Number.

What are we doing? Upon discovering this incident, Richards blocked the unauthorized party from further accessing our network. We worked with forensic investigators to confirm that the unauthorized user no longer had access to Richards's email environment. Additionally, we have taken steps to enhance our data security measures to prevent the occurrence of a similar event in the future, including forced password changes and additional detection safeguards to our corporate network environment.

What you can do. Despite the fact that the unauthorized user may not have been successful in actually obtaining any files, we would like to offer you a complimentary 24-month membership of complimentary identity monitoring services provided by Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
*You have until **<<b2b_text_6(activation deadline)>>** to activate your identity monitoring services.*
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

For More Information. If you have questions, please call TFN, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding U.S. Holidays. Please have your membership number ready.

Sincerely,

Richards Industrials

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. **You may contact the nationwide credit reporting agencies at:**

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 680-7289

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.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. 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. 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. You can place a freeze and lift a security freeze on your credit report free of charge.

You may contact the Federal Trade Commission (FTC) 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 contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

For Iowa residents, State law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Pro-Tem, Inc. dba PTI Systems is located at 2525 South Shore Boulevard, Suite 401 League City, TX 77573.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.