METRO WIRE ROPE CORPORATION

SINCE NOVEMBER 21, 1977

February 27, 2018

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

RE: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

Metro Wire Rope Corporation ("Metro Wire") is writing to inform you of a recent incident that may impact the security of certain information. We are providing information on the incident, steps we have taken and ways in which you can protect your information, should you feel it appropriate to do so.

What Happened? On November 27, 2017, we learned of phishing emails being sent from a Metro Wire employee's email account to our vendors. We immediately changed the employee's email account credentials and launched an investigation into this activity to determine what happened. Firms with a focus on cybersecurity issues were retained to assist with our own internal investigation. The investigation determined that the Metro Wire employee received a phishing email containing an attachment with credential stealing capabilities. The employee's email account credentials were captured through the malicious attachment and were used by unknown individual(s) to gain unauthorized access to the employee's email account. While the only unauthorized activity observed in the account was the transmission of phishing emails, we cannot rule out the possibility of the unknown individual(s) gaining access to any specific email or attachment in the account. In an abundance of caution, the entire account underwent a programmatic and manual review to identify the personal information that may be contained within the account.

What Information Was Involved? Through the programmatic and manual review of the employee email account, we determined on January 16, 2018, that the following information related to you may have been contained in the employee's email account at the time it was accessed by the unknown individual(s): <<ClientDef1(first and last name, [credit card information/financial account data/driver's license number])>>

What We Are Doing. Metro Wire takes the security of your information very seriously. In addition to taking the steps detailed above to terminate the unauthorized access, Metro Wire is providing you with information on how to protect against identity theft and fraud, as well as access to free identity monitoring services. Since discovering the phishing emails, we have been working to ensure the security of our systems and confirm the nature and scope of this incident. Metro Wire is committed to continuing employee training designed to help them identify and properly report potential email phishing scams. Finally, we are providing notice of this event to state Attorneys General as required.

What You Can Do. Please review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*, which contains instructions on how to activate free identity monitoring services, as well as information on what you can do to better protect yourself against the possibility of identity theft and fraud should you feel it is appropriate to do so.

For More Information. We sincerely regret any inconvenience or concern this may have caused. If you have questions that are not answered in this letter, please contact Kroll at 1-866-775-4209, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time, excluding major holidays.

Sincerely,

Jack J. Gibbons
President

9741WP-0218

Steps You Can Take to Protect Against Identity Theft and Fraud

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. 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, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

You have until **May 28, 2018** to activate your identity monitoring services.

Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze/place-credit-freeze

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

For North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 0 Rhode Island resident(s) may be impacted by this incident. **For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, 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 Fair Credit Reporting Act, 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 Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above.