March 4, 2016

Notice of Data Breach

Dear ISCO Employee:

On March 3, 2016, ISCO Industries, Inc. ("ISCO") discovered that certain sensitive ISCO employee information was compromised as a result of a criminal act. We take the privacy and security of your personal information very seriously. This notice is intended to provide you with important information so you can take appropriate action to protect your interests.

What Happened

On March 2, 2016, an employee in our human resources department received an email from someone posing as a senior executive at ISCO asking for ISCO's 2015 IRS Form W-2 data. A W-2 is the form that ISCO distributes to all of its employees and income taxing authorities at the end of each January. Because the email appeared to come from within ISCO, the employee gathered the requested W-2 data in electronic format and transmitted the information by return email. Shortly thereafter, we realized that an outside third party had fraudulently disguised his email address as that of an ISCO senior executive, and that our employees' W-2 data had been unwittingly sent to that outside third party.

Compromised Information

The compromised information includes employee social security numbers, addresses, and 2015 compensation and tax withholding information. ISCO has no reason to believe employee credit card, banking, birthdate, telephone, driver's license, health insurance, or medical information was obtained. We have been notified by some employees that individuals may have attempted to log on to their accounts with private tax preparers using this information.

As soon as ISCO discovered this security breach, it acted to notify and cooperate with the FBI, the IRS, and the Louisville Metro Police Department. ISCO learned that this criminal act is part of a larger scam attempting to file false tax returns with the hope of diverting employee tax refunds. If you have already filed your tax returns, there is a likelihood that the IRS would reject any duplicate, fraudulent return. If you have not yet filed your tax returns, we recommend completing the attached IRS Form 14039 Identity Theft Affidavit and faxing it to the IRS (fax instructions are included on the form).

Identity Protection Services

ISCO has retained LifeLock, Inc. (www.lifelock.com) to provide identity theft protection services for each employee affected free of charge. Lifelock will provide individual email or text notifications if it detects someone is trying to open a fraudulent credit card or borrow money in your name. We have purchased a 12-month membership for all U.S. employees. Information on how to set up an individual account is attached to this notice.

Fraud Prevention Tips

ISCO wants to make you aware of steps you may take to guard against identity theft or fraud.

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 identity theft to proper law enforcement authorities, your state attorney general, the Internal Revenue Service, and the Federal Trade Commission. To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

You should also notify your accountant or tax preparation agency (H&R Block, Jackson Hewitt, etc.) of this security breach and ask them about ways to prevent fraudulent submission of information to the IRS and state and local governments. The IRS has internal security measures in place, so refund wiring instructions which do not include your address or the address of your financial institution, or contain an address which differs from the one on your W-2 form may cause the IRS to send you clarifying correspondence before processing a refund. Please pay attention to any correspondence from the IRS and respond promptly to any inquiry.

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 a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the tree national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(800) 685-1111/Fraud Division: (800) 525-6285
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742/Fraud Division: (888) 397-3742
www.experian.com
535 Anton Blvd., Suite 100
Costa Mesa, CA 92626

TransUnion
(8000) 916-8800/Fraud Division: (800) 680-7289
www.transunion.com
P.O. Box 6790
Fullerton, CA 92834

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 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. 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.

In some U.S. states, you have the right to put a security freeze on your credit file. 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 reporting agency. (Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $5 to place, lift or remove the security freeze.) 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.

Questions About This Notice

For further information and assistance, please contact Karlie Burton at 502-614-3660 or karlie.burton@isco-pipe.com between the hours of 8:00am and 5:00pm Eastern, Monday through Friday.

Please be assured that we will continue to monitor this situation and address promptly any further issues. To this end, we will endeavor to provide you with updated information as it becomes available.

Sincerely,

Christopher Feger
Chief Administrative Officer
ISCO Industries, Inc.