PO Box 128, 817 West Main Street, Brownsville, WI 53006

April 25, 2016

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
ATTN: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Dear Attorney General Joseph Foster:

Pursuant to N.H. Rev. Stat. § 359-C:20(I)(b), we are writing to notify you of a breach of security involving 48 New Hampshire residents.

NATURE OF THE UNAUTHORIZED DISCLOSURE

On April 16, 2016, a Michels Corporation ("Michels") employee was targeted by an isolated email phishing scam in which an individual outside of Michels impersonated a Michels executive requesting certain information for Michels employees. The result of the cyber-scam was that certain information related to current and former employees who would have received a W-2 for 2015 was disclosed. The information involved in this incident includes names, addresses, Social Security numbers, earnings and withholding information for anyone who was issued a W-2 for the 2015 tax year. None of our systems were breached and no other information was accessed or obtained.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

As a result of this incident, 48 residents of the State of New Hampshire have been affected. Each of these residents will receive a notice of this breach in writing via U.S. mail to be sent on April 27, 2016. Enclosed is a sample copy of the notice that is being provided to the individuals affected.

STEPS WE ARE TAKING RELATED TO THE INCIDENT

We were first notified of the incident on April 18, 2016, when the manager of Payroll and Union Benefits notified management of the disclosure on April 16, 2016. The manager immediately notified and met with Finance, HR, IT, and legal teams to determine the nature and scope of the incident, and our investigation is ongoing. We have contacted state and federal law enforcement and are fully cooperating with them. In addition, we are reviewing our internal policies and procedures to prevent any similar incident from happening again in the future. All affected employees are being offered two years of identity protection services through LegalShield Inc. at no charge to the affected individuals.

OTHER NOTIFICATION AND CONTACT INFORMATION

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

David Stegeman
Chief Legal Officer
MICHELS Corporation
office: 920.924.4328
fax: 920.583.4187
DStegema@michels.us

Sincerely,

David Stegeman
Chief Legal Officer
Encl: Sample Breach Notification Sent to Affected Individuals

Sample Breach Notification Sent to Affected Individuals

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

<<Date>>

<<First Name>> <<Last Name>>
<<Street Address>>
<<City>>, <<State>> <<Zip>>

NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>:

We value you as an employee of Michels and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that involves your personal information and some steps you can take to help protect yourselves.

We apologize for any frustration or inconvenience this may cause you. This cybercrime is something that has impacted all Michels' personnel, and we are all in this together.

As a result, we have arranged for you to receive identity protection services for two years at no cost to you. Instructions for enrolling and activation in these services can be found in the "What We Are Doing" Section below and in the IDShield Enrollment and Activation Steps enclosure.

WHAT HAPPENED

This matter is still under investigation but we want to report this preliminary information. On April 16, 2016, a Michels employee was targeted by an isolated email phishing scam in which an individual outside of Michels impersonated a Michels executive requesting certain information for Michels employees. The result of the cyber scam was that certain information related to current and former employees who would have received a W-2 for 2015 was disclosed.

None of our systems were breached and no other information was accessed or obtained. We are truly sorry for the occurrence of this incident and we are doing everything we can to work with our people to prevent any similar incident from happening in the future. Federal law enforcement has been notified about this incident. We will also continue to investigate this incident.

WHAT INFORMATION WAS INVOLVED

The information involved in this incident includes names, addresses, Social Security numbers, earnings and withholding information for anyone who was issued a W-2 for the 2015 tax year.

WHAT WE ARE DOING

Michels values your privacy and deeply regrets that this incident occurred. We are conducting a thorough review of the events surrounding this cybercrime, and will notify you if there are any significant developments. We have implemented additional security measures designed to prevent a recurrence of such an event, and to protect the privacy of Michels' valued employees. In addition, we have contacted state and federal law enforcement and will be fully cooperating with them. We will also be working with outside subject matter experts in this investigation and to avoid any similar incidents.

To help protect your information, Michels is offering you two years of free identity protection services through LegalShield, Inc. These services help detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This service is completely free and it will not impact your credit score. For more information, and how to enroll in this free service, please see the "What You Can Do" Section below.

WHAT YOU CAN DO

Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information.

Identity Protection Services. In addition, Michels has arranged with LegalShield to provide you with identity protection services for two years, at no cost to you. The LegalShield. package, known as IDShield, provides you with the following benefits:

- Identity Protection and Privacy Monitoring,
- Security Monitoring,
- Identity Consultation Services,
- Identity Restoration

To take advantage of this offer, you must enroll within 90 days from receipt of this letter.

We've included enrollment instructions in the IDShield Enrollment and Activation Steps enclosure. We strongly encourage you to enroll in this free service. If, however, you choose not to, we encourage you to monitor your credit reports and other financial records for fraudulent transactions as well as review the information included in the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information.

FOR MORE INFORMATION

For further inquiries concerning this notification or assistance, please contact the specially created Michels Employee Information Center at 888-871-2201 between 7:00 a m. and 5:00 p.m.(CST).

We are very sorry to have to deliver this message. We are all victims of this cybercrime and we want to assure you that we will cooperate fully with the FBI and seek prosecution once the perpetrator(s) are found and charged.

Sincerely,

Pat Michels
CEO
Enclosure(s): Steps You Can Take to Further Protect Your Information
IDShield Enrollment and Activation Steps

Steps You Can Take to Further Protect Your Information

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.

To file a report with the FTC, go to www ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Reports filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

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 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 three 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	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

Fraud Alert

We recommend 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 www.annualcreditreport.com.

Security Freeze

In some US 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 of credit reporting agencies listed above. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee to place, lift or remove the security freeze, which may vary by state. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Complaint Form with the FTC, there may be no charge to place 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.

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 Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

Federal Trade Commission: You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit www ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at www ftc.gov/bcp/edu/microsites/idtheft/.

For Maryland residents: Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at www.oag.state md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or calling 410-576-6491.

For North Carolina residents: North Carolina residents may wish to review information provided by the North Carolina Attorney General, Consumer Protection Division at www.ncdoj.gov, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

For California residents: California residents may wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.

Reporting of identity theft and obtaining a policy report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Taxes

Some of the information affected by this incident could be used to file a fraudulent tax return. If you believe you are the victim of tax fraud or that somebody has filed or accessed your tax information, you should immediately contact the IRS or state tax agency as appropriate.

For Federal Taxes: The IRS requires that each individual report the problem to them. The IRS will not financially penalize you even if they paid a fraudulent refund. Accordingly, as an additional measure of precaution, we recommend you (and, if applicable, your spouse or domestic partner) complete IRS Form 14039 and then mail or fax that form to the IRS. A copy of that form can be obtained by going to https://www.irs.gov/pub/irs-pdf/f14039.pdf. You may also call the IRS at 800-908-4490 (Identity Theft Hotline) to learn whether you are a victim of this fraudulent scheme. For additional information from the IRS about identity theft, you may visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

For State Taxes: There may be similar resources and forms for each state, so we recommend that you contact your state department of revenue directly for more information. Additional information on how to contact your state department of revenue may be found by going to http://www.taxadmin.org/state-tax-agencies.

IDSHIELD ENROLLMENT AND ACTIVATION STEPS

IDShield

Your IDShield (a product of LegalShield) membership is a powerful thing.

ENROLL NOW (either method)

- Go to: www.legalshield.com/[redacted] and click on the "Signing Up" link starting Wednesday, April 27, 2016.
- Call the specially created Michels Employee Information Center at (888) 871-2201 to request a paper application (an email address is needed to enroll for services).

THE IDSHIELD℠ MEMBERSHIP INCLUDES:

Privacy Monitoring

Monitoring your name, SSN, date of birth, email address (up to 10), phone numbers (up to 10), driver license & passport numbers, and medical ID numbers (up to 10) provides you with comprehensive identity protection service that leaves nothing to chance.

Security Monitoring

SSN, credit cards (up to 10), and bank account (up to 10) monitoring, sex offender search, financial activity alerts and quarterly credit score tracking keep you secure from every angle. With the family plan, Minor Identity Protection is included and provides monitoring for up to 8 children under the age of 18.

Consultation

Your identity protection plan includes 24/7/365 live support for covered emergencies, unlimited counseling, identity alerts, data breach notifications and lost wallet protection.

Full Service Restoration

Complete identity recovery services by Kroll Licensed Private Investigators and our $5 million service guarantee ensure that if your identity is stolen, it will be restored to its pre-theft status.

ACTIVATE

- After you enroll go to www myidshield.com and create an account with your membership number to identify and enter information you want guarded.
- Feel free to call an IDShield Advisor at (888) 494-8519 after you complete the enrollment process with any questions about Identity Theft.