MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Jeffrey J. Boogay
Office: 267-930-4784
Fax: 267-930-4771
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

October 9, 2019

INTENDED FOR ADDRESSEE(S) ONLY
VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

We represent The McKeogh Company ("McKeogh"), 4 Tower Bridge, Suite 225, 200 Barr Harbor Drive, West Conshohocken, PA 19428, and write to notify your office of an incident that may affect the security of some personal information relating to approximately one hundred fifty (150) New Hampshire residents. The investigation into this event is ongoing and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, McKeogh does not concede that this is a reportable event under New Hampshire law and does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about June 26, 2019, McKeogh learned that one of its employees failed to delete or return certain documents relating to clients of McKeogh after his last day of work. Upon learning of this information, McKeogh immediately began the process of identifying which documents were retained by the former employee. Through its investigation, McKeogh determined that files containing information related to certain AMETEK employees participating in its pension plans were taken by the now-former employee, prior to his departure. This employee was authorized to work on these files prior to his departure but did not have permission to take the files. McKeogh worked to secure the documents and recovered the information from the former McKeogh employee. McKeogh also obtained an Affidavit confirming that the information was not retained, transferred to a third-party, or used for any other purposes. McKeogh, therefore, has no reason to believe the information was retained by the employee for a criminal or improper purpose. Further,

McKeogh had a third-party forensic firm search the former employee's computer and external data storage devices to confirm nothing was retained and transferred to a third-party.

Although McKeogh confirmed that the employee returned the data and did not share its contents with any third parties, McKeogh confirmed the files contained names, dates of birth, and Social Security numbers that McKeogh utilized to prepare benefit pension plan information.

Notice to New Hampshire Residents

On or about October 9, 2019, McKeogh began mailing written notice of this incident to all affected individuals, which includes approximately one hundred fifty (150) New Hampshire residents. Written notice to the individuals is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, McKeogh moved quickly to investigate and respond to the incident, assess the security of its systems, and notify potentially affected individuals. McKeogh is also working to implement additional safeguards and review its policies and procedures related to safeguarding information in its care.

While the information was returned to McKeogh and McKeogh is not aware of any attempted or actual misuse of the information, in an abundance of caution, McKeogh is providing access to credit monitoring services for twenty-four (24) months, through Kroll, a division of Duff & Phelps, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, McKeogh is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. McKeogh is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,

Jeffrey Boogay of
MULLEN COUGHLIN LLC

JJB/gcl
Enclosure

EXHIBIT A

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

The McKeogh Company ("McKeogh") is writing to inform you of a recent event that may impact the security of some of your personal information. McKeogh was in possession of your information in its role in the administration of AMETEK, Inc.'s ("AMETEK") pension plans. While we are unaware of any actual or attempted misuse of your personal information, we are providing you with information about the incident, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On or about June 26, 2019, McKeogh learned that one of its employees failed to delete or return certain documents relating to clients of McKeogh after his last day of work. Upon learning of this information, McKeogh immediately began the process of identifying which documents were retained by the former employee. Through its investigation, McKeogh determined that files containing information related to certain AMETEK employees participating in its pension plans were taken by the now-former employee, prior to his departure. This employee was authorized to work on these files prior to his departure but did not have permission to take the files. McKeogh worked to secure the documents and recovered the information from the former McKeogh employee. McKeogh also obtained an Affidavit confirming that the information was not retained, transferred to a third-party, or used for any other purposes. McKeogh, therefore, has no reason to believe the information was retained by the employee for a criminal or improper purpose. Further, McKeogh had a third-party forensic firm search the former employee's computer and external data storage devices to confirm nothing was retained or transferred to a third-party.

What Information Was Involved? Although McKeogh confirmed that the employee returned the data and did not share its contents with any third parties, we also confirmed the files contained your name, date of birth and Social Security numbers that McKeogh utilized to prepare benefit pension plan information.

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities and we take this incident very seriously. As part of our ongoing commitment to the security of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to help prevent this from happening in the future.

Based on our investigation and efforts taken in response to this incident, we are confident that all AMETEK employee information was returned and not misused. However, as an added precaution, we are also offering you complimentary access to twenty-four (24) months of identity monitoring services through Kroll. We encourage you to activate these services, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Protect Your Information* for additional information on these services.

What You Can Do. 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. You may review the enclosed *Steps You Can Take to Protect Your Information*, which contains information on what you can do to better protect against the possibility of identity theft and fraud should you feel it is appropriate to do so. You may also activate the free identity monitoring services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our toll-free dedicated assistance line at 1-866-775-4209, Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Amanda Notaristefano

Mandy Notaristefano, F.S.A.
Principal
The McKeogh Company

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

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

*You have until **January 5, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Monitor Your Accounts

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.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, 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); TTY: 1-866-653-4261. 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. 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 report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. You may also write to us at 4 Tower Bridge, Suite 225, 200 Barr Harbor Drive, West Conshohocken, PA 19428.

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.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are five (5) Rhode Island residents impacted by this incident.