James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

March 8, 2018

INTENDED FOR ADDRESSEE(S) ONLY

VIA U.S. MAIL AND EMAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
Email: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent ABM Industries Incorporated, One Liberty Plaza, 7th Floor, New York, New York 10006 ("ABM"), and are writing to notify your office of an incident that may affect the security of personal information relating to certain Washington residents. By providing this notice, ABM does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about August 1, 2017, ABM discovered that it had become the target of a phishing email campaign and that several employees had clicked on the phishing email and entered their credentials. ABM immediately took steps to secure the employees' email accounts and launched an in-depth investigation to determine whether any sensitive information was accessed or acquired.

ABM subsequently determined, with the help of outside computer forensic investigators, that an unknown actor had gained access to the ABM employees' email accounts. While ABM's investigation into the contents of the email accounts is ongoing, on December 21, 2017, ABM determined, after an in-depth programmatic and manual review of the contents of the email accounts, the types of protected information contained in the email accounts and to which individuals the information relates, and immediately launched a review of its files to ascertain address information for the impacted individuals. This included engagement of a vendor to

provide advanced address look-up services to ensure notice would be mailed to the person's most recent address on record.

While there is no evidence that the individual(s) accessed or acquired personal information from the employees' email accounts, access to the information contained therein could not be ruled out. The email account may have contained the name, date of birth, address, Social Security Number, financial account information, and medical information of the affected Washington residents.

Notice to Washington Residents

ABM provided notice to approximately four hundred and thirty (430) Washington residents on November 13, 2017 and December 19, 2017. However, ABM identified an additional six hundred and seventy (670) Washington residents during its continued investigation into this incident. ABM is now providing notice of this incident to the Washington Attorney General because the November 13, 2017 and December 19, 2017 notice to impacted individuals did not exceed the threshold required for notice to the Attorney General's Office. Written notice has been provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

ABM is providing all potentially affected individuals access to 1 free year of credit and identity monitoring services, including identity restoration services, through Kroll, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, ABM is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. ABM is also providing written notice of this incident to other state regulators as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4798.

Very truly yours,

James E. Prendergast of
MULLEN COUGHLIN LLC

Exhibit A

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Re: Notice of Data Breach

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

We are writing to inform you of a recent event that may affect the security of your personal information. You previously provided ABM Industries Incorporated or one of its subsidiaries ("ABM") with certain personal information, and the security of your information is important to us. While we are unaware of any actual or attempted misuse of your personal information, out of an abundance of caution, we are providing you with information about a recent incident, steps we are taking in response, and steps you can take to protect against fraud, should you feel it is appropriate.

What Happened? On or about August 1, 2017, we discovered that ABM had become the target of a phishing email campaign. For background, phishing is a type of electronic attack where outside individuals impersonate a trusted person or company to obtain information or install dangerous software. Several ABM employees had clicked on the phishing emails and entered their credentials. As is our protocol, we immediately took steps to secure these employees' email accounts and launched an in-depth investigation to determine whether any sensitive information was accessed or acquired.

We subsequently determined, with the help of outside computer forensic investigators, that an unknown actor had gained access to certain ABM email accounts. ABM determined, after a programmatic and manual review of the contents of the affected email accounts, the types of protected information contained in the affected email accounts and to which individuals the information relates.

What Information Was Involved? While we currently have no evidence that the unauthorized individual or individuals actually accessed or acquired your information, we have confirmed that your <<ClientDef1>><<ClientDef2>> (data elements affected) accessible within the affected email accounts.

What We Are Doing. We take the security of information in our care very seriously. Since discovering this event, we have been working diligently with third-party forensic investigators to determine what happened and what information was accessible to the unknown actor. This has involved a programmatic and manual data review process. It is important to us to let you know this happened and are providing notice of this event to you, and to certain regulators and consumer reporting agencies.

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 **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **June 4, 2018** to activate your identity monitoring services.*

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

What You Can Do. In the event you are not already receiving credit monitoring and wish to do so, or wish to have additional credit monitoring, you can enroll and receive the free credit monitoring and identity restoration services we are offering by visiting the site above or by calling the number below to request credit monitoring through the mail. You can also review the enclosed Privacy Safeguards Information for additional information on how to better protect against identity theft and fraud.

For More Information. Information security is a top priority to us. Should you have any questions about the content of this letter, ways you can better protect yourself from the possibility of identity theft, please call 1-833-210-8120 between 9:00 am and 6:00 pm ET, Monday through Friday, excluding major holidays.

Sincerely,

ABM Industries Incorporated

PRIVACY SAFEGUARDS

In addition to enrolling to receive the free monitoring and restoration services we are offering to you, we encourage you to remain vigilant against incidents of identity theft and financial loss by reviewing your account statements and monitoring your credit reports for suspicious activity. Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
800-680-7289
www.transunion.com

At no charge, you can also have these credit bureaus place a "fraud alert" on your credit file. A "fraud alert" will tell creditors to take additional steps to verify your identity prior to granting credit in your name; however, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the credit bureaus verify your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your files. You may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on your credit report.

You can also place a "security freeze" on your credit file that prohibits a credit bureau from releasing any information from your credit report without your written authorization but may delay, interfere with, or prevent the timely approval of any requests for new credit. If you have been a victim of identity theft, and provide the credit bureau with a valid police report, the credit bureau cannot charge to place, lift, 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. If you incur a cost to place a security freeze, please let us know. You must contact each of the credit bureaus separately to place a security freeze on your credit file:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents please call 1-800-349-9960)
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
PO Box 2000
Chester, PA 19022-2000
1-888-909-8872
www.transunion.com/securityfreeze

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. **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 violators. 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 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 101 Rhode Island residents may be impacted by this incident.

Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. This notice was not delayed as the result of a law enforcement investigation.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] 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 can help you determine if it's an indicator of identity theft.

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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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.