ABM
Building Value

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

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

RE: Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

We are writing to inform you of an event that may affect the security of some of your personal information. You provided ABM Industries Incorporated or one of its subsidiaries, including GCA Services Group, Inc. ("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 the event, steps we have taken in response, and steps you can take to protect against fraud should you feel it is appropriate.

What Happened?

On or around June 14, 2018, ABM was alerted to suspicious activity related to certain employee email accounts. ABM immediately launched an investigation into the incident to determine the full nature and scope of what occurred. Through its detailed and exhaustive investigation, ABM confirmed that an unknown actor gained access to certain ABM employee email accounts as the result of a phishing attack against the email accounts. Phishing is a type of electronic attack where outside individuals impersonate a trusted person or company to obtain information, such as email credentials. The affected employees' email credentials were changed, and the email accounts have been secured.

A leading forensic investigation firm was immediately retained to assist with ABM's investigation into what happened and what information contained within the email accounts may be affected. The investigation determined that the accounts at issue experienced unauthorized access between January 8, 2018 and August 7, 2018. The contents of the accounts were reviewed through an in-depth manual and programmatic process to determine what sensitive data may have been accessible. On December 26, 2018, we confirmed the identities of the individuals who may have had information accessible as a result of the incident and promptly launched a review of our files to ascertain address information for the impacted individuals.

What Information Was Involved?

While we currently have no evidence that your information was subject to actual or attempted misuse, we have confirmed that your <<ClientDef1(name and [Data Elements])>><<ClientDef2([Data Elements])>> were contained within the affected employee email accounts. This does not necessarily mean that your personal information was actually reviewed by any third parties, simply that it was accessible to be opened and potentially reviewed by the unknown actor.

What We Are Doing.

We take the confidentiality, privacy, and security of information in our care very seriously. Upon learning of this incident, we took steps to secure the affected email accounts and to find out what happened and what information was accessible to the unknown actor. It is important to us to let you know this happened and we are providing notice of this incident to you, and to law enforcement, certain regulators and consumer reporting agencies.

We have secured the services of Kroll to provide identity monitoring at no cost to you for one year. More information on these services can be found in the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud."

ABM has an ongoing commitment to data security and privacy. This ongoing commitment starts with ABM's Board of Directors, which requires regular cyber-security updates from our Chief Information Officer on, among other things, current and future security threats and the state of ABM's use of security enhancing technology and outside security vendors. We are continually exploring and implementing new technologies and vendors with increasing emphasis on strengthening our security capabilities. For example, since 2017, ABM has employed the use of malware detection software, implemented new technology, such as multi-factor authentication, and has recently implemented third-party managed security services, with coverage 24 hours per day, 7 days per week, to better enable detection and prevention of unauthorized activity on our systems. Our commitment to data security and privacy also includes company-wide anti-phishing and cyber-security training, which we have been providing to our employees and which we regularly update to better prevent future such incidents.

What You Can Do.

You may review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud". You may also enroll to receive the free identity theft protection and identity restoration services described above.

For More Information.

We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-231-3357, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

Sincerely,

ABM Industries Incorporated

Steps You Can Take to Protect Against Identity Theft and Fraud

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 5, 2019 to activate your identity monitoring services.

Membership Number: [redacted]

To receive credit services by mail instead of online, please call 1-833-231-3357.

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
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
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
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
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.

ABM has an ongoing commitment to data security and privacy. This ongoing commitment starts with ABM's Board of Directors, which requires regular cyber-security updates from our Chief Information Officer on, among other things, current and future security threats and the state of ABM's use of security enhancing technology and outside security vendors. We are continually exploring and implementing new technologies and vendors with increasing emphasis on strengthening our security capabilities. For example, since 2017, ABM has employed the use of malware detection software, implemented new technology, such as multi-factor authentication, and has recently implemented third-party managed security services, with coverage 24 hours per day, 7 days per week, to better enable detection and prevention of unauthorized activity on our systems. Our commitment to data security and privacy also includes company-wide anti-phishing and cyber-security training, which we have been providing to our employees and which we regularly update to better prevent future such incidents.

What You Can Do.

You may review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud". You may also enroll to receive the free identity theft protection and identity restoration services described above.

For More Information.

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

Sincerely,

ABM Industries Incorporated

Steps You Can Take to Protect Against Identity Theft and Fraud

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 5, 2019 to activate your identity monitoring services.
Membership Number: [redacted]

To receive credit services by mail instead of online, please call 1-???-???-????.

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
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
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
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
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 ABM at Attn: Legal Department, One Liberty Plaza, 7th Floor, New York, New York 10006.

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, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 134 Rhode Island residents impacted by this incident.

Kroll.

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.