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

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Dear <<Name 1>>:

We write to notify you of a recent data privacy incident involving our subsidiary, The Affiliated Group ("TAG"). This notification provides details on the incident, the investigation, and steps we have and are taking in response to the incident.

On or about March 28, 2018, we confirmed that an earlier phishing email incident involving TAG resulted in unauthorized access to one (1) TAG employee email account. Upon learning of the phishing email incident, we immediately disabled the account and reset all account passwords. Thereafter we worked with third-party forensic investigators to determine what happened, and whether sensitive information may have been accessible as a result of this incident. With the assistance of the third-party investigators, we learned that an unauthorized actor gained access to the one TAG employee email account. Unfortunately, the investigation was unable to determine which emails, if any, were specifically accessed as a result of this incident. The only confirmed unauthorized activity identified was the use of the account to send phishing emails in an attempt to harvest user credentials. Since the investigation was unable to rule out access to any specific email or attachment, we undertook a programmatic and manual review of the contents of the account.

After a thorough and detailed review of the contents of the accessed account, we subsequently determined that personal and/or protected health information relating to your customers, including their first and last name, and some combination of Social Security number, medical record number, limited treatment information and/or subscriber ID was potentially accessible. A limited number of financial account information was also identified in the review. To date we have no evidence to suggest that the information was subject to actual or attempted misuse as a result of this incident.

We take the privacy of the information in our care very seriously. Upon discovering this incident, we have been working diligently with third-party forensic investigators to determine what happened and what information was potentially accessible to the unauthorized actor. This has involved a time consuming, programmatic and manual data review process. This review process is complete and we are notifying you now that we have been able to identify the sources of the accessible information. We have also taken steps to further increase our security awareness to reduce the likelihood of a similar event from occurring in the future.

This event may result in the imposition of a legal obligation on the Covered Entity who provided the information to TAG to provide notice of this event to the individuals whose information was accessible, to the Department of Health and Human Services as well as certain state agencies. However, we are offering to notify impacted individuals and regulators on your behalf. In order to notify the impacted individuals and regulators, we are asking that you provide us with your approval within fourteen (14) days of the date of this notice, by email request sent to CMeier@thecmigroup.com. Please contact us directly to confirm whether you wish TAG to notify your customers and regulators on your behalf. You can also contact us at this email address to receive a list of potentially affected individuals who are affiliated with your organization.

Again, we take the security of personal information in our system very seriously and we apologize for any inconvenience or concern this incident may have caused you. If you have any questions or concerns, please do not hesitate to contact us at (972) 862-4232.

Sincerely,

Chris Meier, Esq.

General Counsel &
Chief Compliance Officer
to The CMI Group, Inc., parent company of TAG

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

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Re: Notice of Data Breach

Dear <<Name 1>>:

We are writing regarding a data privacy incident that may involve your personal and/or protected health information. We take this incident seriously and are providing you with information and access to resources so that you can better protect your information, should you feel it is appropriate to do so.

What happened? On or about March 28, 2018, we at The Affiliated Group ("TAG"), confirmed that an earlier phishing email incident in November 2017 involving TAG resulted in unauthorized access to one TAG employee email account. Upon learning of the phishing email incident, we immediately disabled the account and reset all account passwords. Thereafter, we worked with third-party forensic investigators to determine what happened and whether sensitive information may have been accessible. With the assistance of the investigators, we learned that an unauthorized person gained access to the one TAG employee email account. Unfortunately, the investigation was unable to determine which emails, if any, were specifically accessed as a result of this incident. The only confirmed unauthorized activity identified was the use of the account to send phishing emails in an attempt to obtain user credentials. Since the investigation was unable to rule out access to any specific email or attachment, we undertook a programmatic and manual review of the contents of the account.

What information was involved? The thorough review of the account involved a programmatic and manual process that looked at every email and attachment in the account to identify the personal and protected health information present, verify whom the accessible information belonged to, and obtain a last known address to direct the notice of the incident. Through this lengthy and time-consuming process, our investigation determined that your name and some combination of protected and/or personal information including, Social Security number, driver's license number/state identification number, and financial account or payment card number was potentially accessible in attachments contained within the email account. This information would have been shared with TAG as part of the collection services TAG performs on behalf of certain medical providers and other organizations. We currently have no evidence that any of your information was subject to actual or attempted misuse as a result of this incident.

What is TAG doing? We take the privacy of your information in our possession seriously. We have taken steps to further increase our security awareness to reduce the likelihood of a similar event from occurring in the future. We are providing notice of this event to you, which includes access to free credit monitoring services (discussed further below). We also notified certain regulators as required.

What you can do. You can enroll in and receive the free credit monitoring and identity restoration services we are offering through TransUnion®. You can also review the enclosed Steps You Can Take to Protect Your Information for additional details on how to better protect against potential misuse of your information.

For more information. If you have additional questions, please call our dedicated assistance line at (844) 801-5967, Monday through Friday, 8:00 a.m. to 8:00 p.m. CT (excluding US holidays).

TAG takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Chris Meier, Esq.

General Counsel &
Chief Compliance Officer
TAG

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.

- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.

- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, 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.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you 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. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/center.html	freeze.transunion.com

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting 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); and TTY: 1-866-653-4261. 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement. **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 11 Rhode Island resident(s) may be impacted by this incident. **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 a 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. 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.

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

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

We are writing regarding a data privacy incident that may involve your personal and/or protected health information. We take this incident seriously and are providing you with information and access to resources so you can better protect your information, should you feel it is appropriate to do so.

What happened? On March 28, 2018, we at The Affiliated Group ("TAG"), confirmed that an earlier phishing email incident in November 2017 involving TAG resulted in unauthorized access to one TAG employee email account. Upon learning of the phishing email incident, we immediately disabled the account and reset all account passwords. Thereafter, we worked with third-party forensic investigators to determine what happened and whether sensitive information may have been accessible. With the assistance of the investigators, we learned that an unauthorized person gained access to the one TAG employee email account. Unfortunately, the investigation was unable to determine which emails, if any, were specifically accessed as a result of this incident. The only confirmed unauthorized activity identified was the use of the account to send phishing emails in an attempt to obtain user credentials. Since the investigation was unable to rule out access to any specific email or attachment, we undertook a programmatic and manual review of the contents of the account.

What information was involved? After a thorough and detailed review of the contents of the accessed account, our investigation determined that your name and some combination of protected and/or personal information—including Social Security number, medical record number, limited treatment information and/or subscriber ID—was potentially accessible in attachments contained within the email account. This information would have been shared with TAG as part of the collection services TAG performs on behalf of certain medical providers and other organizations, such as <<*Entity*>>. We currently have no evidence that any of your information was subject to actual or attempted misuse as a result of this incident.

What is TAG doing? We take the privacy of your information in our possession seriously. We have taken steps to further increase our security awareness to reduce the likelihood of a similar event from occurring in the future. We are providing notice of this event to you, which includes access to free credit monitoring services (discussed further below). We also notified your creditor, <<*Entity*>>, which TAG was acting as collections agent for, and we are notifying certain regulators as required.

What you can do. You can enroll in and receive the free credit monitoring and identity restoration services we are offering through TransUnion®. You can also review the enclosed *Steps You Can Take to Protect Your Information* for additional details on how to better protect against potential misuse of your information.

For more information. If you have additional questions, please call our dedicated assistance line at (844) 801-5967, Monday through Friday, 8:00 a.m. to 8:00 p.m. CT (excluding US holidays).

TAG takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Chris Meier, Esq.

General Counsel &
Chief Compliance Officer
TAG

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.

- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.

- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised, and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, 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.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you 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. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/center.html	freeze.transunion.com

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting 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); and TTY: 1-866-653-4261. 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement. **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 11 Rhode Island resident(s) may be impacted by this incident. **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 a 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. 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.