July 5, 2018

Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Dear Attorney General MacDonald,

Pursuant to N.H. Rev. Stat. Ann. § 359-C:20(I)(b), we are writing to notify you of a data breach involving information stored on systems maintained by Cushman and Wakefield ("C&W") that affected one New Hampshire resident.

Nature of the Security Breach

In or about February 2018, C&W was alerted to the existence of phishing emails sent to certain C&W employees, through which unauthorized parties were able to obtain the user credentials for C&W employees who received and opened the emails and supplied their user credentials. Since learning of this issue, C&W has acted quickly to address the breach.

Based on our investigation to date, we believe that unauthorized parties may have been able to access information contained in certain employees' C&W accounts, including the account user's name, emails, social security number and/or bank account number. We believe the unauthorized parties may have been able to access this information for certain individuals beginning on approximately February 26, 2018 through approximately March 1, 2018.

Residents Affected

On July 5, 2018, C&W mailed written notice to the one New Hampshire resident whose personal information was affected pursuant to N.H. Rev. Stat. Ann. § 359-C:20(I)(a). A copy of that notice is attached hereto as Exhibit A.

Steps Taken

After learning of this incident, C&W worked quickly to identify potentially affected accounts and to prevent any further unauthorized access to employees' personal information. These efforts included temporarily locking the accounts of affected users, forcing password resets, and identifying and blocking access to C&W systems from suspected malicious IP addresses. C&W has also retained the services of a firm specializing in data breaches to assist in its response.

C&W is reporting this matter to law enforcement where appropriate. C&W is also providing no-cost credit monitoring services to the affected employees. C&W provides training to its employees regarding awareness and detection of phishing attacks, and will continue to do so in the future.

Contact Information

For more information, or if you have any additional questions or concerns about this incident, you may contact our outside counsel Adam Fee, of Milbank, Tweed, Hadley & McCloy LLP, at 212-530-5101.

EXHIBIT A

July 5, 2018

{NAME}
{Mailing Address 1}
{Mailing Address 2}

NOTICE OF DATA BREACH

We are writing to notify you of an issue that may involve your personal information stored on systems maintained by Cushman and Wakefield ("C&W"). The privacy and protection of our employees' information is a matter we take very seriously, and we are providing this notice to inform you about the incident and to call your attention to some steps you can take to help protect yourself.

What Happened?

C&W was recently alerted to the existence of phishing emails sent to certain C&W employees, through which unauthorized parties were able to obtain the user credentials for C&W employees who received and opened the emails and supplied their user credentials. Since learning of this issue, C&W has acted quickly to address any potential data breach.

What Information Was Involved?

Based on our investigation to date, we believe that unauthorized parties may have been able to access information contained in certain employees' C&W accounts, including the account user's name, emails, social security number and bank account number. We believe the unauthorized parties may have been able to access this information beginning on approximately February 26, 2018 through approximately March 1, 2018.

What We Are Doing.

After learning of the issue, C&W immediately began working to identify potentially affected accounts and to prevent any further unauthorized access to employees' personal information. In addition to our internal efforts to address this issue, we will be providing notice of this incident to law enforcement and state regulators as required. As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months:

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-676-0379 and a

dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com using the following redemption code: {RedemptionCode}.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may be required in order to activate your monitoring options.

What You Can Do.

We recommend that you review financial account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and to continue to monitor financial account statements for unusual activity going forward. We further recommend that, as a general practice, you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies.

You can also review the enclosed Additional Information Regarding Identity Theft Protection supplement, which includes guidance on steps you can take to better protect against the possibility of fraud and identity theft.

For More Information.

For more information, or if you have any additional questions or concerns about this incident, you may contact us at 212-713-6851.

Additional Information Regarding Identity Theft Protection

Monitoring Your Accounts

Credit Reports. 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.

Fraud Alerts. 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. 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 19106
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freezes. 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. To find out more on how to place a security freeze, you may 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 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/	freeze.transunion.com

Additional Information

You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-IDTHEFT (1-877-438-4338); and TTY: 1-866-653-4261. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For Oregon Residents: You may report any instance of suspected identity theft to law enforcement, including the Oregon Attorney General or the Federal Trade Commission. Those agencies can be contacted at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
http://www.doj.state.or.us

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft