THE CARLYLE GROUP

1001 Pennsylvania Avenue, NW • Suite 220 South • Washington, DC 20004-2505
Tel (202) 347-2626 • Fax (202) 347-1818

April 4, 2019

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Breach Pursuant to N.H. Rev. Stat. Ann. § 359-C:20

To Whom It May Concern:

In accordance with the above-referenced provision of New Hampshire law, I write to inform you of an information security incident affecting approximately four individuals who we believe to be New Hampshire residents.[1]

Carlyle is a global investment firm that provides investment-related services primarily to certain institutional and other financially sophisticated investors. Carlyle has engaged a third-party vendor to develop, host and manage an online repository by which Carlyle's limited partners (including legal entities, eligible employees, and certain other individuals) can access certain investment-related documents and other information.

On or about February 19, 2019, after Carlyle reported performance issues with the repository, the vendor notified Carlyle that it had begun an investigation of a series of unauthorized attempts to gain access to the platform that supports the repository. Carlyle immediately took action to protect individuals' data—including shutting off this potential unauthorized access to the repository, invalidating all passwords, and undertaking our own investigation in coordination with our vendor and its outside security and forensics experts. On March 6, 2019, Carlyle determined—based on information provided by the vendor—that the incident may have resulted in unauthorized acquisition of certain personal information on the platform between on or about January 30, 2019 and on or about February 12, 2019.

Based on our investigation to date, we believe that the data involved was generally limited to basic business contact information of some users. For a small subset of users, the data may have also included information defined as "personal information" under N.H. Rev. Stat. Ann. § 359-C:19(IV).[2] We have not seen any evidence of misuse of this data.

Upon learning of the incident, Carlyle took immediate steps to protect individuals by investigating the incident, eliminating and preventing any further unauthorized access, and

enhancing our security and monitoring measures. We have also contacted law enforcement and worked closely with our vendor and its outside forensic experts throughout this process. Upon determining that the attack may have resulted in access to certain personal information, we also started working immediately to notify potentially impacted individuals and offer assistance, including offering free credit monitoring services for a two-year period.

In addition to the e-mail notices and assistance already provided to potentially affected individuals, we plan to send an un-redacted version of the attached letter to these individuals via first-class mail by April 5, 2019.[3] As indicated in the attachment, the notification to individuals includes: (1) a description of the incident and the type of personal information at issue; (2) the actions taken by Carlyle to protect personal information from further unauthorized access; (3) Carlyle's address and a toll-free phone number to call for further information and assistance; (4) information on how the individual may enroll in free credit monitoring and other complimentary services arranged by Carlyle; (5) information about how to place a fraud alert or security freeze on a credit report; (6) the toll-free numbers and addresses for the major consumer reporting agencies; (7) the toll-free number, address, and website for the Federal Trade Commission; and (8) advice that directs the individual to remain vigilant by reviewing account statements and monitoring free credit reports.

If you have any questions or need further information regarding this incident, please do not hesitate to contact me.

Sincerely,

Catherine Ziobro
Chief Compliance Officer and Managing Director
The Carlyle Group
(202) 729.5597
catherine.ziobro@carlyle.com

Enclosure

THE CARLYLE GROUP

1001 Pennsylvania Avenue, NW • Suite 220 South • Washington, DC 20004-2505
Tel (202) 347-2626 • Fax (202) 347-1818

April 5, 2019

[Recipient Name]
[Recipient Address]
[Recipient City/State]

NOTICE OF DATA BREACH

The safety and security of your personal data is of critical importance to The Carlyle Group, and a responsibility we take very seriously. Between February 21, 2019 and March 17, 2019, we notified you by e-mail of a recent security incident involving Carlyle's vendor that hosts Carlyle's investor reporting site, [redacted]. This letter is a written notice regarding the same security incident.

What Happened?

On or about February 19, 2019, after Carlyle reported performance issues with [redacted], the vendor notified Carlyle that it had begun an investigation of a series of unauthorized attempts to gain access to the platform that supports [redacted]. We immediately took action to protect your data—including shutting off this potential unauthorized access to [redacted], invalidating all passwords, and undertaking our own investigation in coordination with our vendor and its outside security and forensics experts. On March 6, 2019, Carlyle determined—based on information provided by the vendor—that the incident may have resulted in unauthorized acquisition of certain personal information on the platform between on or about January 30, 2019 and on or about February 12, 2019.

What Information Was Involved?

Based on our investigation to date, we believe that the data accessed was generally limited to basic business contact information – such as [redacted] of some users. [redacted] may also have been accessed, but we have no indications that [redacted] were accessed.

For a small subset of users who participated in our internal coinvestment program, including you, the data accessed may have also included [redacted] In addition, we have indications that unauthorized access of [redacted] may have occurred, but we do not believe the data accessed included [redacted]. We have not seen any evidence of misuse of this data.

What Are We Doing?

Upon learning of this incident, we took immediate steps to investigate the incident, eliminate and prevent any further unauthorized access, and work with the vendor to enhance the security and monitoring measures for [redacted]. We have also contacted law enforcement and worked closely with our vendor and its outside forensic experts throughout this process. Upon determining that the incident may have resulted in access to certain personal information, we also notified potentially impacted individuals via their email address on file.

We are offering you and other affected individuals participating in our internal coinvestment program two years of complimentary credit monitoring and identity protection services through Experian IdentityWorksSM Credit 3B. You may sign up for this service by following the instructions provided in our prior communication to you on March 17, 2019. If you did not receive this communication or have any questions about the Experian services, please contact us at privacy@carlyle.com.

What Can You Do?

Regardless of whether you elect to enroll in the identity-theft protection service, we strongly recommend that you remain vigilant and regularly review and monitor all of your credit history to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your account statements and notify your financial institution if you suspect any unauthorized activity. **Attachment A** contains more information about steps you can take to protect yourself against fraud and identity theft.

As a safeguard, if you have not changed your [redacted] password after February 19, 2019, we will also require that you change your password the next time you log into [redacted]. In an abundance of caution, you should consider changing your password for any third-party sites for which you used the same password as [redacted]. Additional information on password security from the U.S. Federal Trade Commission (FTC) can be found at https://www.consumer.ftc.gov/blog/2018/03/its-national-password-day.

For More Information.

We sincerely regret that this incident occurred, and we apologize for any inconvenience that may have been caused by this incident. If you have any questions about this notice or the incident, please feel free to contact Catherine Ziobro at catherine.ziobro@carlyle.com.

Sincerely,

Catherine Ziobro
Chief Compliance Officer and Managing Director
The Carlyle Group
(202) 729.5597
catherine.ziobro@carlyle.com

ATTACHMENT A

ADDITIONAL INFORMATION

To protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your State's attorney general, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three credit reporting agencies below:

Equifax:	Experian:	TransUnion:
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: Consider contacting the three major credit reporting agencies at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts one year, but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, please be aware 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.

Placing a credit freeze is free. To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

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, 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.); and
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or http://www.marylandattorneygeneral.gov/.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or http://www.riag.ri.gov/. You may also file a police report by contacting local or state law enforcement agencies.