carlysle ENGINEERING, INC. THE FIRE PROTECTION PEOPLE
249 Oceana Way • Norwood, MA 02062 • Tel: 617-522-6650 • Fax: 617-522-9021

Via Email

May 14, 2026

Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

RE: Notification of Data Breach

Dear Office of the New Hampshire Attorney General Representative:

Pursuant to N.H. Rev. Stat. Ann. § 359-C:20(I)(b), we are notifying the New Hampshire Office of the Attorney General of a data breach, affecting approximately six (6) New Hampshire residents.

On March 23, 2026, Carlysle Engineering, Inc. ("Carlysle") discovered that a cybercriminal had launched an attack on Carlysle's primary file server, which encrypted the files on the server. Upon discovery of the attack, Carlysle's information technology ("IT") administrator immediately engaged OCD Tech, LLC ("OCD Tech"), a well-known cybersecurity recovery and investigation firm, and cybersecurity legal counsel to investigate the incident and coordinate efforts with our IT administrator.

By the afternoon of March 23rd, OCD Tech identified a ransom note and list of encrypted files on the primary file server. According to OCD Tech's investigation, a relatively new ransomware group was responsible for the attack and the cybercriminal was able to exfiltrate some of Carlysle's data on the affected server. Based on its investigation, OCD Tech informed us that the incident began on March 23, 2026, and ended on the same day after OCD Tech updated the security system and shut down the affected connections.

On March 23, 2026, OCD Tech initiated incident response procedures, including containment and forensic investigation. OCD Tech also conducted a thorough and diligent review of all files that we were able to confirm were impacted in order to identify the individuals affected by this incident, along with their mailing addresses. This review was finalized on April 23, 2026. Based upon OCD Tech's investigation, the cybercriminal's access to identifiable data was limited to a single part of our network, which included human resources data, such as W2 reports and scans of driver's licenses. While the types of information affected will vary by person, the personal information maintained in the affected files generally included the following: name, address, date of birth, Social Security Number, and driver's license number/state-issued ID number.

Carlysle is taking a number of steps to reduce the likelihood of future unauthorized access to its systems, including implementing recommendations received from OCD Tech, including updating the firewall.

Carlysle is notifying all affected individuals by first class U.S. mail on May 14, 2026. A template copy of the notification being sent to current and former Carlysle employees and beneficiaries who were affected by this breach is attached. Carlysle is also notifying relevant state authorities of this cyberattack.

Carlysle is offering all affected individuals complimentary identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include all of the following: twenty-four (24) months of CyberScan® monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

I want to assure you that Carlysle takes its obligation to protect the privacy and confidentiality of its employees' personal information very seriously, and while no business is 100% secure in this day and age, Carlysle is working to evaluate ways in which it can reduce the likelihood of future unauthorized access to its systems. If you have any questions, please contact me by phone at 1-617-522-6650 or by email at maurer@carlysle.net.

Sincerely,

Chip Maurer
General Manager
Carlysle Engineering, Inc.
249 Oceana Way
Norwood, MA 02062

carlysle
ENGINEERING, INC.
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

Enrollment Deadline: August 14, 2026

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

May 14, 2026

RE: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

We have discovered that Carlysle Engineering, Inc. ("Carlysle," "we," "us") was the victim of a ransomware attack. The attack affected our human resources data, and some of that data may have included some of the personal information we maintain about you as a current or former Carlysle employee or named beneficiary of a current or former Carlysle employee. We are writing to explain what happened, how we have responded, and what you can do to protect your personal information.

Here is what happened:

On March 23, 2026, Carlysle discovered that a cybercriminal had launched an attack on Carlysle's primary file server, which encrypted the files on the server. Upon discovery of the attack, Carlysle's information technology ("IT") administrator immediately engaged OCD Tech, LLC ("OCD Tech"), a well-known cybersecurity recovery and investigation firm, and cybersecurity legal counsel to investigate the incident and coordinate efforts with our IT administrator.

By the afternoon of March 23rd, OCD Tech identified a ransom note and list of encrypted files on the primary file server. According to OCD Tech's investigation, a relatively new ransomware group was responsible for the attack and the cybercriminal was able to exfiltrate some of Carlysle's data on the affected server.

Based on its investigation, OCD Tech informed us that the incident began on March 23, 2026 and ended on the same day after OCD Tech updated the security system and shut down the affected connections.

How we responded:

As explained above, on March 23, 2026, OCD Tech initiated incident response procedures, including containment and forensic investigation. OCD Tech also conducted a thorough and diligent review of all files that we were able to confirm were impacted in order to identify the individuals affected by this incident, along with their mailing addresses. This review was finalized on April 23, 2026.

While no business can be 100% secure, we are working to implement recommendations received from OCD Tech to reduce the likelihood of a future cyberattack, including updating the firewall.

Types of information involved:

Based upon OCD Tech's investigation, the cybercriminal's access to identifiable data was limited to a single part of our network, which included human resources data, such as W2 reports and scans of driver's licenses. While the types of

information affected will vary by person, the personal information maintained in the affected files generally included the following: name, address, date of birth, Social Security Number, and driver's license number/state-issued ID number.

Protection of your information:

We are providing written notice to all individuals that we have identified as having information potentially affected by this incident. Included with this notice is a "Reference Guide," which provides useful information regarding how to protect your identity, including obtaining copies of your credit report and implementing credit freezes. We encourage you to review the Reference Guide closely.

In addition, we are offering you twenty-four (24) months of identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-788-9712, going to https://app.idx.us/account-creation/protect, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9am - 9pm Eastern Time. **Please note the deadline to enroll is August 14, 2026. Your unique enrollment code is <<Enrollment Code>>.**

For more information:

Carlysle takes its obligation to protect the privacy and confidentiality of our employees' personal information very seriously and we deeply regret that this breach occurred. If you have any questions, you may contact Chip Maurer, by phone at 1-617-522-6650 or by email at maurer@carlysle.net.

Sincerely,

Chip Maurer
General Manager
249 Oceana Way
Norwood, MA 02062

Reference Guide

Review Your Account Statements. We encourage you to remain vigilant by reviewing your account statements. If you believe there is an unauthorized charge on your card, please contact your financial institution or card issuer immediately. The payment card brands' policies provide that cardholders have zero liability for unauthorized charges that are reported in a timely manner. Please contact your card brand or issuing bank for more information about the policy that applies to you.

Order A Free Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and about fraud alerts and security freezes:

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

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 2002 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. For more information on security freezes, you may contact the three nationwide consumer reporting agencies, or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	1-800-349-9960	www.equifax.com/personal/credit-report-services/
Experian	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze/center.html
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-888-909-8872	www.transunion.com/credit-freeze

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)
- Social Security Card, pay stub, or W2
- 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.

For Massachusetts Residents. You have the right to obtain any police report filed in regard to this 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. You may also place a security freeze on your credit reports, free of charge. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/resources/individuals/consumer-issues/technology

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)-274-4400
www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For North Carolina Residents.

You can also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000
www.ncdoj.gov