MAYNARD
COOPER GALE

Sarah Glover
DIRECT 205.254.1877
EMAIL sglover@maynardcooper.com

January 22, 2021

Attorney General Gordon McDonald
Office of Attorney General
33 Capitol Street
Concord, NH 03301

Re: Recent Security Incident

Dear Attorney General McDonald,

I am writing to let you know that our client, Clarus Corporation ("Clarus" or "Company"), experienced a security incident that impacted the personal information of eight New Hampshire residents, who are former employees of Clarus.

The Company supplied notice to affected individuals in December to let them know what happened, and to inform them of available resources to further monitor and protect their personal information. We are providing notice to your office pursuant to N.H. Rev. Stat. § 359-C:19, *et seq*.

On October 4, 2020, Clarus discovered that it had fallen victim to a ransomware attack after detecting encrypted files on its network. The Company immediately reported the incident to law enforcement. The Company also engaged outside experts through its insurance carrier to conduct an investigation, which concluded this month.

The forensic investigation identified September 23, 2020 as the earliest observed date of unauthorized activity within the Clarus network. Thereafter, the threat actor used compromised login credentials to execute malicious tasks that were used to exfiltrate data and deploy the ransomware. A review of the exfiltrated files uncovered the personal information of 8 New Hampshire residents. This information included the individuals' name and social security number. One year of complimentary credit monitoring and identity theft protection services were extended to the affected individuals. A copy of the individual notice is enclosed.

Please do not hesitate to let me know if you have any questions or would like additional information.

Sincerely,

Sarah Glover

December 22, 2020

Re: Security Incident

Dear former employee

I hope this letter finds you well during these difficult times. I am writing to let you know about a security incident that Black Diamond Equipment experienced at the beginning of October that temporarily disrupted our IT network. We have been working with outside experts to understand how it happened, and what impact it had on our systems. That investigation is now complete.

Our experts have determined that the network outage resulted from a malware infection. Unfortunately, we have learned that some files were downloaded from our network during the incident that contained personal information we have on file for you. **The outside experts we hired to investigate the situation have uncovered no evidence that your information has been misused**. However, we want to make sure you have the right resources at your disposal to take the appropriate precautions you feel are needed to protect your identity.

What Happened?
An unknown individual accessed and downloaded files from the Black Diamond network on or about October 4, 2020. A review of these files revealed that your personal information would have been available within one or more of these files. Searches by our experts did **not** uncover any of these files online.

What Information Was Available?
The information our experts observed varied. Generally speaking, these files may have included your social security number and/or driver's license number. If you would like to know exactly what information of yours, if any, was found, please send a request to privacyquestion@bdel.com.

What We Are Doing?

Security is extremely important to us. We have added some additional network requirements to strengthen the security of our environment heading into 2021. We will continue to monitor access to our systems for unauthorized activity and are committed to protecting the information we maintain throughout our organization.

What You Can Do?
We want to reassure you that we have no indication that any of your personal information has been misused. However, out of an abundance of caution, we have included information on several resources that are available to protect your identity. All of these are simple, effective ways to detect the unauthorized use of your identity. We are also offering a complimentary, one year, subscription to an identity monitoring service. Please reach out to privacyquestion@bdel.com if you would like to receive this service.

We are extremely apologetic this happened, and for any inconvenience this may cause you. Please do not hesitate to reach out to us at privacyquestion@bdel.com if you have any questions or concerns. This is the e-mail address we have specifically created to field any questions about this incident.

Sincerely,

Aaron Kuehne

IDENTITY PROTECTION RESOURCES (U.S.)

1. Review your Credit Reports. We recommend that you remain vigilant by monitoring your credit reports. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months.

2. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is only necessary to contact one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact each of the three national credit reporting bureaus listed above in writing to place the freeze. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your Social Security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus

must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze.

4. Monitor Your Accounts. We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective financial institution.

5. You can obtain additional information about the steps you can take to avoid identity theft and more information about fraud alerts and security freezes from the Federal Trade Commission (FTC). You may contact the FTC, Consumer Response Center at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.

***

Iowa Residents: You can report suspected identity theft to law enforcement, the FTC, or to the Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-888-777-4590, https://www.iowaattorneygeneral.gov/.

Maryland Residents: You can obtain additional information about preventing identity theft from the FTC, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, https://www.ftc.gov/, and the Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (410) – 528-8662, https://www.marylandattorneygeneral.gov/.

Massachusetts Residents. You have the right to obtain any police report filed regarding this incident. You also have the right to file and obtain a copy of a police report if you are the victim of identity theft.

New York Residents: You can obtain additional information about identity theft prevention and protection from the New York State Attorney General, The Capitol, State Street and Washington Avenue, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.

North Carolina Residents: You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, https://ncdoj.gov/.

Oregon Residents: You can report suspected identity theft to law enforcement, the FTC, or the Oregon Office of the Attorney General at: Oregon Department of Justice, 1162 Court St NE, Salem, OR 97301, 1-800-850-0228, https://www.doj.state.or.us/.