Troutman Pepper Hamilton Sanders LLP
600 Peachtree Street NE, Suite 3000
Atlanta, GA 30308-2216

troutman.com

**Charles E. Peeler**
D 404.885.3409
charles.peeler@troutman.com

May 28, 2021

**VIA OVERNIGHT MAIL AND EMAIL (NDAG@ND.GOV)**

Attorney General Wayne Stenehjem
600 E. Boulevard Ave., Dept. 125
Bismarck ND 58505
(701) 328-2210

**Re: Incident Notification**

Dear Attorney General Stenehjem:

I represent Clark Equipment Company d/b/a Doosan Bobcat North America ("DBNA"), and as follow-up to my initial notification on February 23, 2021 to your office, I am writing to update you about the data security incident that may have exposed personal information of North Dakota residents. While we have no reason to believe that a North Dakota resident's information has been misused, we are contacting you and the individuals directly to provide information on what occurred, and how we are responding. The breach involved six thousand six hundred and ninety-three (6693) North Dakota residents as of the date of this letter.

## I. Description of Event

DBNA was notified on January 20, 2021 by its IT vendor of a cybersecurity event involving a different client of the IT vendor that resulted in unauthorized access to three of DBNA's file servers. Our IT vendor immediately took steps to secure the file servers, retained a forensics investigation firm and conducted an investigation into the nature and scope of the security incident. The investigation determined that, between January 3, 2021 and January 22, 2021, an unknown actor was able to access personal information. After DBNA itself learned of the attack, DBNA further hired the services of its own investigator to analyze the personal information that may have been impacted. Further investigation indicated that the attack specific to DBNA's servers occurred on or around January 13, 2021.

The investigation has revealed that the attack was conducted by an unknown person or group that initially leveraged a compromised email account associated with a different client of the IT vendor. We understand from our IT vendor that it appears the perpetrator performed privilege escalation and lateral movement, and gained access to DBNA's servers. DBNA's investigation is ongoing, but we have confirmed that three servers belonging to DBNA were compromised, and currently have no evidence to believe any additional DBNA servers have been affected.

troutman pepper

## II. Remedial Steps Taken in Response to the Breach

DBNA takes the protection of personal information very seriously. Upon learning of this incident, we worked diligently to understand what happened and remedy the situation. Our IT vendor took steps to remove the unknown actors from all systems, implemented a global password reset, and deployed additional security for privileged accounts. DBNA also took steps to improve security and worked with our IT vendor to implement multifactor authentication for all employee email accounts and install new software and security applications to detect and prevent suspicious activity on its servers and networks. DBNA also notified law enforcement.

The confidentiality, privacy, and security of information is one of our highest priorities and we take this incident very seriously. Accordingly, as part of our ongoing commitment the protection and proper use of information, we are working to review our existing policies and procedures, to implement additional safeguards, and to provide additional training to our employees on data privacy and security.

## III. Notification to the Affected Residents

Attached as Exhibit A to this letter is a sample notice that will be sent to affected individuals in North Dakota following this notification to you. The letter advises the residents to monitor their credit reports and accounts; recommends that they place a fraud alert on their credit files and provides instructions on how to do so; and provides contact information for DBNA and encourages them to contact DBNA with any additional questions.

Please rest assured that DBNA takes individuals' privacy very seriously, and will continue to work diligently to protect individuals' personal information. If you have any questions or require any additional information regarding this incident, please do not hesitate to contact me.

Sincerely,

Charles E. Peeler

Enclosures/Attachments

**EXHIBIT A**

**Individual Notice Letter**

[___], 2021

**{Name}**
**{Address}**
**{Address}**

**An Important Message**

Dear **{Name}**:

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident. While we have no reason to believe your personal information has been misused, out of an abundance of caution, we are contacting you directly to let you know what occurred, how Doosan Bobcat North America is responding and what precautionary measures you can take.

**What Happened**

On or about January 20, 2021, Clark Equipment Company d/b/a Doosan Bobcat North America ("DBNA," "we," "us," "our") was notified by its IT vendor of a cybersecurity event involving a different client of the IT vendor that resulted in unauthorized access to three of DBNA's file servers. Our IT vendor immediately secured the file servers, retained a forensics investigation firm and conducted an investigation into the nature and scope of the security incident. The investigation determined that, between January 3 and January 22, 2021, an unknown actor was able to access personal information. DBNA also hired its own investigator to analyze the personal information that may have been impacted by this incident.

**What Information Was Involved**

The personal information may have included information you provided to DBNA, such as {Listed Specific Categories of Personal Information}. To date, DBNA has not received any reports of actual or attempted misuse of your information. Nevertheless, we are notifying you of this incident to help you take precautionary measures to prevent fraud or identity theft.

**What We Are Doing**

DBNA takes the protection of personal information very seriously. Upon learning of this incident, we worked diligently to understand what happened and remedy the situation. Our IT vendor took steps to remove the unknown actors from all systems, implemented a global password reset, and

deployed additional security for privileged accounts. DBNA also took steps to improve security and worked with our IT vendor to implement multifactor authentication for all employee email accounts, including installing new software and security applications to detect and prevent suspicious activity on its servers and networks. DBNA also notified law enforcement.

The confidentiality, privacy, and security of information is one of our highest priorities and we take this incident very seriously. Accordingly, as part of our ongoing commitment to the protection and proper use of your information, we are working to review our existing policies and procedures, implement additional safeguards, and provide additional training to our employees on data privacy and security. We are also notifying state regulators as required.

**What You Can Do**

Please review the document titled *Steps You Can Take to Help Protect Your Personal Information,* which is enclosed with this letter. This document describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. As a precautionary measure, we recommend you remain vigilant by reviewing account statements and monitoring free credit reports, and take preventive actions, including those detailed in *Steps You Can Take to Help Protect Your Personal Information.*

**For More Information**

Protecting you and your personal information is important to us. We sincerely apologize for any inconvenience and concern that this incident may cause. Should you have any questions regarding this notice, including questions regarding your particular records, please do not hesitate to contact us 8:00 am to 5:30 pm Central Time, Monday through Friday excluding major US holidays at (855) 537-2117.

DOOSAN BOBCAT NORTH AMERICA

**EXHIBIT A**

**IDENTITY THEFT PREVENTION INFORMATION**

**FTC and State Attorneys General Offices:** You may take steps to protect yourself against potential misuse of data that has been the subject of a data security incident. The Federal Trade Commission discusses several steps, including obtaining and reviewing your credit report, filing a "fraud alert" and requesting a "credit freeze". The most current and detailed information is available online (for answers to the questions below, see https://www.ftc.gov/faq/consumer-protection), but if you are not able to access the linked material, you may also contact the FTC by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, or by toll-free number, 1-877-FTC-HELP (382-4357) or 1-877-ID-THEFT (438-4338).

1. What are the steps I should take if I'm a victim of identity theft?
2. What is a fraud alert?
3. What is a credit freeze?
4. Should I apply for a new Social Security number?
5. What are the steps I should take if I'm a victim of identity theft?
6. What is a fraud alert?
7. What is a credit freeze?
8. Should I apply for a new Social Security number?

**For Maryland residents**: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

**For New York residents:** The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

**For Connecticut residents:** You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

**For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

**Fraud Alert and Security Freezes:** A fraud alert tells creditors to take reasonable steps to verify your identity, including calling you before opening new accounts or changing your existing accounts. A fraud alert may be placed or removed at no cost to you. An initial fraud alert stays active for 90 days. To request a fraud alert, you will need to contact one of the following credit reporting agencies (see the FTC materials for further details). The credit reporting agency is required to notify the other two credit reporting agencies, who will also place a fraud alert on your credit file. You will then receive letters from all of them with instructions on how to obtain a free copy of your credit report from each.

Equifax Information Services, LLC
P.O. Box 740241 Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
National Consumer Assistance
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022
1-800-916-8800
www.transunion.com

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

If you observe evidence of attempts to open fraudulent accounts and you have a copy of a police report reporting that you are experiencing identity theft, then you may also request a 7-year fraud alert. Be aware that placing a fraud alert does not always prevent new accounts from being opened or prevent a takeover of your existing accounts, so you should monitor any alerts sent to you by the credit monitoring companies. Also, be aware that a company may not be able to immediately extend credit to you if your identity can not be verified at the time you are applying for credit. You should consider providing a mobile telephone number when placing any fraud alert if you have one.

You also can contact the nationwide credit reporting agencies to place a security freeze to restrict access to your credit report altogether. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization.

However, 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, mortgages, employment, housing, or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022
(888) 909-8872

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
1. Social Security Number;

1. Date of birth;
1. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
1. Proof of current address such as a current utility bill or telephone bill;
1. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
1. 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;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report or to remove the security freeze altogether, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

**Monitor Credit Reports and Accounts:** When you receive your credit reports, you should look them over carefully and consider taking the steps recommended by the FTC. For example, look for accounts you did not open. Additionally, look for inquiries from creditors that you did not initiate. And finally, look for personal information that you do not recognize. Also, you should monitor your accounts for suspicious activity. If you see anything you do not understand, call the credit reporting agency or provider of your account at the telephone number on the credit report or account statements. If you do find suspicious activity on your credit reports, you may call your local police or sheriff's office and may be able to file a police report of identity theft and obtain a copy of the police report. Potentially, you may need to give copies of the police report to creditors to clear up your records. You may also make a report to the FTC.

**Obtain Free Credit Reports:** Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report regularly for at least the next one to two years. Each of the three credit reporting agencies is required to provide you with a free credit report, at your request, once every 12 months. You may visit www.annualcreditreport.com, the only Web site authorized by Equifax, Experian and TransUnion for this purpose, to find out more. This website also provides instructions for making a request by phone (1-877-322-8228) or by mailing a request on a form supplied at the site and sending it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. For Colorado, Georgia, Maine, Maryland, Massachusetts, New

Jersey, Puerto Rico, and Vermont residents, you may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Rights under the Fair Credit Reporting Act**

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 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 https://files.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.

**Reporting of identity theft and obtaining a police report:**

Customers have the right to file a police report if they 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, customers 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.

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.