Crown Equipment Corporation
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
DB-09190

1_0000002

0000002

40 S Washington St
New Bremen, OH 45869

<<NAME>>
<<ADDRESS>>
<<CITY, STATE ZIP>>

August 8, 2024

Re: Notification of Data Breach / Cybersecurity Incident

Dear <<NAME>>,

As you may know, Crown Equipment Corporation ("Crown," "our," or "we") was recently the victim of a cyberattack and an unauthorized third party obtained limited access to our information technology (IT) environment. The purpose of this letter is to inform you that the privacy of certain personal data related to you and your family members, could have potentially been compromised during the incident. However, as we have previously communicated with you, we are highly confident **that any data impacted by this incident (including personal data) will not, and cannot, be misused in any way**.

We recognize that cybersecurity is a significant concern in today's world, and we know that some of our employees and their families have been impacted by other cyberattacks impacting schools, hospitals, and other businesses. Although we are confident that your personal data cannot be misused because of the cybersecurity incident that impacted Crown, we are offering you and your family members free credit monitoring and identity theft protection services as an additional proactive risk mitigation option. **Below are additional details regarding the data incident, as well as information on how to enroll in the credit monitoring and identity theft protection services.**

What Happened?

On June 9, 2024, we discovered that a third party had gained unauthorized access to certain systems in our IT environment. In response, we immediately deployed security measures to contain and mitigate this threat, proactively took systems offline so we could conduct a comprehensive investigation, and retained a leading cybersecurity incident response team to accelerate our recovery efforts. Because of the security controls we implemented prior to this incident, we were able to contain this cyber threat and return to a normal state of business within days (instead of weeks or months).

In addition, as part of our response efforts, Crown proactively notified federal law enforcement agencies, and we received support from them and their cybersecurity partners. Specifically, they undertook their own operations to protect Crown, our employees, and our data. It is because of their efforts that we have high confidence that any Crown data (including personal data) cannot be used for malicious purposes as a result of this cybersecurity incident.

What Information Was Involved?

As part of our investigation into this incident, we know that the main Human Resources (HR) database was not

accessed by any unauthorized third party. However, we discovered that portions of our IT environment that retained certain "census data" on our employees and their family members (e.g., enrollment in our benefits programs), certain data related to workplace injuries, and similar records we retain for administrative purposes, were compromised. These files and records contained sensitive personal data on some of our employees and their family members, such as their names, social security numbers, driver's license numbers, financial account information, and health information. If you would like to know what – if any – personal data related to you or your family members was impacted by this incident, please contact the helpdesk number below.

Why Does Crown Have My Family's Personal Data?

Crown retains HR records on our employees and their family members in order to administer our employee benefit programs (e.g., health and wellness programs). These records often contain personal data for authentication and regulatory compliance reasons. The personal data that we collect for HR-related purposes is not used for any other reason.

What We Are Doing / How We Responded

We take this event, and our information security obligations, seriously and we have taken action to remediate this cybersecurity incident and further enhance our prevention and mitigation efforts. As part of this process, we retained independent third-party IT security consultants to analyze the incident, including our information security tools and our data security methods. As noted above, we proactively notified federal law enforcement and regulatory authorities and we have been in contact with them regarding this incident. Last, our law enforcement and cybersecurity partners engaged in operations to better ensure that any Crown-related data (including personal data) impacted by this cybersecurity incident cannot be misused by the third party responsible for this incident or by anyone else.

Credit Monitoring Services

In response to the incident, we are providing you with access to **Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: **XXXXXXXXXX** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do

Because of the measures and steps implemented by Crown, and our cybersecurity partners, **we have high confidence that your personal data will not, and cannot be misused, because of this cybersecurity incident**. However, there are several steps that you can take to better protect yourself and your personal data more generally. See the attachment for additional information with respect to certain services that may be available to you.

Point of Contact / Call Center

We have established a dedicated call center to answer questions you may have about this incident. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between

the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line at 1-833-XXX-XXXX and supply the fraud specialist with your unique code listed above.

* * * * * * * * * *

We deeply regret that this incident occurred, and we thank you for your attention to this matter.

Sincerely,

John Tate
Senior Vice President

Additional Data Security Information

It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please 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 website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111.
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742.
- TransUnion, PO Box 2000, Chester, PA 19016, https://www.transunion.com, 1-800-916-8800.

When you receive your credit report: (i) review it carefully, (ii) look for accounts you did not open, (iii) look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security Number). You should also look in the "inquiries" section for names of creditors from whom you have not requested credit. You should notify the consumer reporting agencies immediately of any inaccuracies in your report or if you see anything you do not understand. The consumer reporting agency and staff will review your report with you. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

If you are a resident of California, Colorado, Connecticut, Illinois, Iowa, Kansas, Louisiana, Maryland, Massachusetts, New York, North Carolina, Oregon, Rhode Island, or Texas, you may contact and obtain information from your state Attorney General at the following:

- California Department of Justice, Office of Privacy Protection, PO Box 944255, Sacramento, CA 94244-2550, 1-800-952-5225, www.oag.ca.gov/privacy.
- Office of the Attorney General Colorado Department of Law, Ralph L. Carr Judicial Building 1300 Broadway, 10th Floor Denver, CO 80203, 1-720)-508-6000, https://complaints.coag.gov/s/contact-us.
- Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.
- Office of the Illinois Attorney General, 500 South Second Street, Springfield, IL 62701, 1-217-782-1090, https://illinoisattorneygeneral.gov/Contact/.
- Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut St., Des Moines, IA 50319, 1-515-281-5164, https://www.iowaattorneygeneral.gov/.
- Kansas Attorney General's Office, 120 SW 10th, 4th Floor, Topeka, KS 66612, 1-785-296-3751 or 1-888-428-8436.
- Louisiana Department of Justice Office of the Attorney General Consumer Protection Section 1885 N. Third Street Baton Rouge, LA 70802, 1- 225-326-6079, https://www.ag.state.la.us/Contact.
- Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 or 1-410-576-6300, www.marylandattorneygeneral.gov.
- Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/contact-the-attorney-generals-office.
- New York Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.
- North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, 1-919-716-6400 or 1-877-566-7226, https://ncdoj.gov/.
- Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, 1-503-378-4400, https://www.doj.state.or.us/.

- Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, https://riag.ri.gov/.
- Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, 1-512-463-2100, https://www.texasattorneygeneral.gov/contact-us.

Massachusetts. If you are a resident of Massachusetts, you: have the right to file and obtain a copy of a police report; are allowed to place, without charge, a security freeze on your credit reports; and, may contact and obtain information from and/or report identity theft to your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contactus.html.

Rhode Island. If you are a resident of Rhode Island, please note that pursuant to Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

West Virginia. If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a personal identification number ("PIN") that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses listed above.

To request a security freeze, you will need to provide the following information: (i) Your full name (including middle initial as well as Jr., Sr., II, III, etc.), (ii) Social Security number, (iii) Date of birth, (iv) If you have moved in the past five years, provide the addresses where you have lived over the prior five years, (v) Proof of current address such as a current utility bill or telephone bill, (vi) A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.), (vii) If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five 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 lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity 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 one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by

sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act ("FCRA"), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The Federal Trade Commission has published a list of the primary rights created by the FCRA, available at (www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The Federal Trade Commission's list of FCRA rights includes the following:

You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request. Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months. You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days, if you are on welfare, or if your report is inaccurate because of fraud, including identity theft. You have the right to ask for a credit score. You have the right to dispute incomplete or inaccurate information. 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 reports to be provided to employers. You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report. You may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

Note: The delivery of this notice has not been delayed as a result of a law enforcement investigation.