Crown Equipment Corporation
Cybersecurity Incident

Frequently Asked Questions (FAQs)

Last Updated: August 9, 2024

Crown Equipment Corporation ("**Crown**" or "**we**") experienced a cyberattack in June 2024. The following FAQs are intended to address questions or concerns you may have about the incident.

1. What happened?

- In June 2024, Crown experienced a cyberattack and we temporarily suspended our operating systems to investigate and resolve the matter.

- Our internal IT team immediately isolated the malicious activity, deployed security measures to contain and mitigate the threat, and engaged independent security experts to conduct a thorough investigation.

2. What kind of information was accessed?

- As part of this cybersecurity incident, the criminal organization accessed certain files which contained data on some current and former employees, and in some instances, their family members.

3. What types of sensitive personal data was compromised?

- This cybersecurity incident resulted in an unauthorized third party obtaining access to some files that contained sensitive personal data. Crown maintains this personal data to provide health and benefit programs, retirement plans, and in accordance with our record retention obligations.

- Accordingly, the personal data relates to some current and former Crown employees, and in some instances, their family members (e.g., beneficiaries and dependents enrolled in benefit programs).

- Please note that if you are a *current* Crown employee, you will receive a letter from us that describes the types of sensitive personal data that was impacted by this incident.

4. Is my personal data at risk of being misused?

- No. There is no evidence that any data related to this incident, including personal data, has been misused, and we have high confidence that it cannot be misused in the future. Specifically, as part of Crown's response efforts, we proactively notified federal law enforcement agencies, and we received support from them and their cybersecurity partners. 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 misused as a result of this cybersecurity incident.

5. Is Crown offering credit monitoring services? How do I enroll?

- There is no evidence that any data related to this incident, including personal data, has been misused, and we have high confidence that it cannot be misused in the future.

- However, Crown recognizes 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. Accordingly, we are offering you and your family members free credit monitoring and identity theft protection services as an additional proactive risk mitigation option.

- To enroll in this service, go to https://bfs.cyberscout.com/activate, enter your unique Activation Code that was contained in the notice we sent you. If you did not receive a letter, you can get an Activation Code by calling the number below.

- We have a dedicated call center to answer questions you may have about this incident. You can reach the call center at 1-833-531-1952, Monday - Friday, 9:00 am to 9:00 pm (EST).

6. Can current and former Crown employees enroll their family members in the credit monitoring services?

- If you would like additional "enrollment codes" to enroll your immediate family members into these services, please contact our call center at 1-833-531-1952, Monday - Friday, 9:00 am to 9:00 pm (EST) and they will coordinate with us to ensure you have the proper enrollment codes.

7. Why does Crown maintain information on the spouse and children of current and former employees?

- Crown administers certain healthcare, wellness, retirement, and similar benefits programs for our current and former employees. Accordingly, Crown collects and maintains sensitive personal data on the employees enrolled in these programs and on any family members they chose to enroll in these programs (e.g., dependents, beneficiaries).

8. I never received an Activation Code to enroll in the credit monitoring services – what should I do?

- The Activation Code was included in the letters mailed to current employees whose information was affected.

- If you did not receive a letter, or if you lost your letter, please contact our dedicated call center 1-833-531-1952, Monday - Friday, 9:00 am to 9:00 pm (EST) and provide them with your name, mailing address, and telephone

number. The call center will coordinate with Crown to determine whether you and your family members are eligible to enroll in the credit monitoring services.

9. Did Crown report this incident to law enforcement?

- Crown voluntarily notified the Federal Bureau of Investigation (FBI) of this cybersecurity incident, and we have been cooperating with their investigation. We are hopeful that the FBI will capture and prosecute those responsible for this incident.

- In addition, as this incident was occurring, Crown received support from federal law enforcement and regulatory authorities, and their cybersecurity partners. 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 misused as a result of this cybersecurity incident.

10. How did Crown discover the incident?

- Crown had established a comprehensive information security program prior to this incident, and our IT team identified unusual activity occurring within our information networks and systems.

11. How can Crown be sure this type of cyberattack does not happen again?

- Crown implements and maintains a comprehensive information security program, which is one of the reasons we were able to identify this cyberattack and respond to it quickly.

- In addition, we have implemented a broad range of technical, physical, and administrative security controls to safeguard our IT environment, and we will constantly evaluate the sufficiency of these controls against industry standards and reasonably foreseeable threats.

12. Are there any additional steps that I can take to protect myself against fraud and identity theft?

- There is no evidence that any data related to this incident, including personal data, has been misused, and we have high confidence that it cannot be misused in the future.

- However, you should remain vigilant and regularly review your credit card bills, bank statements, and credit reports for any unauthorized activity.

- Promptly report incidents of suspected identity theft or fraud to your local law enforcement agency, the Federal Trade Commission, your state Attorney General, your financial institution, and/or one of the three nationwide consumer reporting agencies.

- Change your passwords regularly, and refrain from using easily guessed passwords and re-using the same passwords for multiple accounts.

13. How can I obtain a free copy of my credit report?

- 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, www.transunion.com, 1-800-916-8800.

14. What should I do if I think my personal data has been misused?

- There is no evidence that any data related to this incident, including personal data, has been misused, and we have high confidence that it cannot be misused in the future. However, if you believe you are the victim of identity theft or have reason to believe your personal data has been misused, you should immediately contact the Federal Trade Commission (FTC) and/or the Attorney General's office in your state.

- The following is the contact information for the FTC: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.