Emmi Roth
Cybersecurity Incident

Frequently Asked Questions (FAQs)

Last Updated: September 7, 2023

Emmi Roth USA, Inc. ("**Emmi Roth**" or "**we**") was subject to a cybersecurity incident in August 2023, and these FAQs are intended to address this incident. The cybersecurity incident impacted Emmi Roth and certain of its affiliates and subsidiaries.

Emmi Roth understands the importance of cybersecurity and protecting your sensitive personal data. From the start, we moved quickly to contain the incident and conducted a thorough investigation with the assistance of leading security experts. We are working hard to ensure that individuals impacted by this incident have answers to questions about their personal data.

1. What happened?

- On August 10, 2023, Emmi Roth was the victim of a cyberattack and an outside group accessed our information networks and systems.
- 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 forensic investigation.

2. What kind of information was accessed?

- As part of this cybersecurity incident, an outside group gained access to certain confidential information in our custody and control, including certain HR files that Emmi Roth maintains on behalf of our own business and on behalf of some of our affiliates and subsidiaries.

3. What type of sensitive personal data was compromised?

- Depending on the company or affiliate/subsidiary current or former employees worked for, the type of personal information involved varies.
- Please note that if you are a *current* employee of Emmi Roth or of certain affiliates and subsidiaries of Emmi Roth, then you will receive a letter/notice from Emmi Roth that describes the types of sensitive personal data that was impacted by this incident.

4. Is Emmi Roth offering credit monitoring services? How do I enroll?

- Emmi Roth will provide complimentary identity-theft monitoring offered through Equifax to the following individuals, to the extent they were impacted by this cybersecurity incident: (i) current and former employees of Emmi Roth, (ii) current and former employees of certain Emmi Roth affiliates and subsidiaries, and (iii) certain family members of these employees.
- To enroll in this service, go to www.equifax.com/activate, enter your unique Activation Code that was contained in the notice we sent you or which you can

obtain by calling the number below; then click “Submit” and follow the four simple steps provided through Equifax’s website.

- In the notification letter, the front page of the enrollment instructions contains the activation code for the employee; the back page contains the activation code for minor children (if applicable). The parent/guardian needs to complete their enrollment first.
- If a spouse, domestic partner or adult child (18 or older) is eligible for coverage, they will need to contact the call center to receive a unique activation code.
- We have a dedicated call center to answer questions you may have about this incident or for assistance enrolling in credit monitoring services. You can reach the call center at 844-709-1704, Monday - Friday, 9:00 am to 9:00 pm (EST).

5. 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 are a former employee, you did not receive a letter, or if you lost your letter, please contact our dedicated call center at 844-709-1704, 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 Emmi Roth to determine whether you and your family members are eligible to enroll in the credit monitoring services.

6. Why does Emmi Roth maintain information on my spouse and children?

- Emmi Roth administers benefits programs for our own employees and some of our former affiliates. In limited circumstances, Emmi Roth collected and maintained sensitive personal data on family members employees chose to enroll in these programs. Out of an abundance of caution, we are going to offer employees or former employees of Emmi Roth and affected affiliates complimentary credit monitoring for their family members.

7. Did Emmi Roth report this incident to law enforcement?

- We 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.

8. I am a supplier or customer of Emmi Roth, was my personal data compromised?

- Emmi Roth does not retain sensitive personal data on our customers, clients, or suppliers, and therefore no such sensitive personal data was involved in this incident.

9. How did Emmi Roth discover the incident?

- Emmi Roth 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.

10. How can Emmi Roth be sure this type of cyberattack does not happen again?

- Emmi Roth 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.

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

- Although there is no evidence that your personal data has been, or will be, misused as a result of this incident, 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 to 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.

12. How can I retain 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 or call toll free at 1-877-322-8228.
- 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.

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

- Although there is no evidence that your personal data has been, or will be, misused as a result of this incident, 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.