JAMECO ELECTRONICS Date:

July 14, 2022

Title: NOTICE OF DATA BREACH

We are writing to inform you about a data incident at Arndt Electronics d/b/a Jameco Electronics ("Jameco") that may have affected your personal information, having been employed by Jameco or one of its affiliates. We take the privacy and security of your information very seriously, which is why we are providing you information about the steps you can take to protect your personal information, and offering credit monitoring services.

What Happened?

On April 23, 2022, Jameco was hit with a ransomware attack in which hackers accessed HR files related to current and former employees of the company. As soon as the incident was discovered, we disabled access to the system and began investigating the incident. We engaged a digital forensics firm to assist with the investigation. We also notified/filed a complaint with the Federal Bureau of Investigation's Internet Crime Complaint Center and will provide whatever cooperation is necessary to hold the perpetrators accountable. Although we are unaware of any actual misuse of your information and notice was not delayed as a result of investigation of law enforcement, we are providing notice to you and other potentially affected employees about the incident, and information you can use to protect yourself against possible identity theft or fraud.

What Information Was Involved?

As an employee or former employee of Jameco, the information on our system may have included your: Full Name, Address, Social Security number, Birthdate, Pay Rate, Emergency contact name, Phone Number, Email Address, Bank Information, Drivers License Number, and Passport Number.

What We Are Doing.

As soon as the incident was discovered, we disabled access to the system. We notified the FBI regarding details of the incident and will provide whatever cooperation is necessary for its investigation. We began investigating the incident and engaged a digital forensics firm to assist with the investigation. We are reviewing in-depth technical policies and procedures to make sure security strategies are in place to

prevent future occurrence. We also are coordinating with a digital forensics firm, external IT specialists and consultants to conduct a root cause analysis and enhance the security of our IT

footprint. We have engaged Norton LifeLock to offer you credit monitoring and related services, as further described below and in the enclosed materials.

What You Can Do.

Although we are unaware of any actual misuse of your information, we strongly recommend that you be proactive in monitoring your accounts and follow the recommendations on the following 2 pages to protect your personal information. You can also take advantage of the 12 months of complimentary credit monitoring we have arranged to provide you through Norton LifeLock. Please refer to the enclosed Benefit Essential Documentation for details of coverage including credit monitoring, identity protection and alerts. You should be receiving an email stating that you are enrolled automatically if we have your email address on file. You can also go to Norton LifeLock (http://norton.com/ebsetup) directly to verify your identity in order to start service. The service starts on the date of this notice and you can use them at any time during the next 12 months.

For More Information.

Further information on how to protect your personal information appear on the following page, and details about the Norton LifeLock services we are offering free of charge are in the enclosed materials. If you have any questions or need assistance, call Employee Benefits Member Services at at LifeLock at 800-607-9174 to speak with a dedicated agent between the hours of 9:00AM and 7:00PM EST, Monday through Friday. LifeLock personnel are standing by to assist you.

We take the protection of your information seriously and sincerely apologize for the inconvenience this incident may cause you. If you have any questions or need further information regarding this incident, please contact us at the phone number we have designated for this matter, (833)740-3137, or send us an email at creditmonitoring@jameco.com.

Sincerely,

James Farrey

James Farrey
CEO, Jameco

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.

You also can contact one of the following three national credit reporting agencies:

Equifax: P.O. Box 105788 Atlanta, GA 30348 1-888-378-4329 www.equifax.com

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

TransUnion: P.O. Box 2000 Chester, PA 19016-2000 1-800-916-8800 www.transunion.com

Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can

take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state.