24631

employee message

[ON KENNEY LETTERHEAD]

Dear XXXXX,

I am reaching out to you personally to share important information about Kenney Manufacturing.

As you may know, Kenney Manufacturing computers experienced a cybersecurity incident on Saturday, November 6, 2021. Our effective safety protocols enabled us to immediately shut down affected equipment and quickly transition to backup systems, limiting disruption to communications, manufacturing, and delivery to a few days.

At present, our in-house professionals and outside consultants have seen no evidence that your personal information was exposed. Further, our outside consultants have been monitoring across the entire internet and have found no evidence that any Kenney employee's personal information was compromised as a result of the November 6 event.

That said, should you receive a call or correspondence that purports to be from our office or ***any*** source claiming to have your personal information, we want you to be prepared.

- Do not engage with the caller/correspondent, and do not get into any detail about whether an attack actually occurred.
- Listen carefully and immediately following the call, make notes about what you were told.
- As soon as possible, share the information with your supervisor or Human Resources.
- We will make sure you receive the information you need to properly respond to the situation.

While we have no evidence that your information was compromised in this attack, we take this situation, and the wellbeing and privacy of our employees, extremely seriously. To that end, we are offering you free credit monitoring services for a period of one year. You will be receiving a packet of information next week with the materials necessary for you to sign up.

To help us successfully counter any future attempt to compromise our systems, we are instituting additional security measures, some of which require changes to our current protocols, including email. We advise our employees to regularly change all your passwords, on all accounts (business and personal), as a best practice.

We have properly informed appropriate governmental authorities and will continue to cooperate fully with law enforcement. Rest assured that If we learn of any additional information pertinent to you, we will share it with you.

We thank you for your continued hard work and digital diligence. Our company would not be what it is without your commitment and dedication to our mission and our success.

Sincerely,

Les Kenney

IF YOUR IDENTITY IS COMPROMISED STEPS YOU CAN TAKE:

- **Local Police Reporting**

  File a report with your local police department.

- **Passwords, Passcodes**

  Change passwords and passcodes on all personal accounts and devices. Often, people will use the same password that they use for one account or device for multiple accounts and/or devices. If you change passwords, this should include your personal social media accounts, online banking accounts, cellphones, tablets, home computers, etc. Best practice is not to use the same password for more than one account or device, nor to "recycle" or reuse passwords that were used in the last several years. If your accounts offer multi-factor authentication, we suggest you enable this for those accounts.

- **IRS**

Complete IRS Form 14039. The form can be found at: https://www.irs.gov/newsroom/tips-for-taxpayers-victims-about-identity-theft-and-tax-returns-2014 and a copy is attached here for your convenience.

You can contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

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.

To file with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **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 http://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 can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Experian	TransUnion	Equifax
(888) 397-3742	(800) 916-8800	(800) 685-1111
www.experian.com	www.transunion.com	www.equifax.com

535 Anton Blvd., Suite 100
Costa Mesa, CA 92626

P.O. Box 6790
Fullerton, CA 92834

P.O. Box 740241
Atlanta, A 30374

- **Fraud Alert**

We recommend 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.

- **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 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 below:

- Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
- TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
- Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three busines 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 PIN or password or both that can be used by you to authorize the removal or lifting of the security freeze.

Massachusetts also offers a resource page on identity theft, which can be found at:

Report identity theft | Mass.gov

And if you have questions or need help, you can call the Attorney General's Consumer Assistance and Response Division at (617) 727-8400.