Good morning,

I'm writing on behalf of Martin Sprocket & Gear, Inc. ("MSG") advising of a data security incident that occurred on or about July 29, 2024. We have attached a copy of the individual notification scheduled to be mailed out Monday, December 16, 2024.

Further details include:

- **The number of affected individuals residing in the State or Maryland:** Four (4)
- **A description of the breach of the security of a system, including when and how it occurred:** In July 2024, the Threat Actor gained access through stolen credentials. Different IP addresses were used going to July 29, 2024. They used an open IP and rented a virtual private server to proxy all traffic. On August 22, 2024, the Threat Actor left various notepad messages on servers, requesting MSG to enter certain chatrooms and use the code. Firewall logs indicated suspicious activity back on July; currently, the log was able to go back to July 14 where the activity was seen. A third-party forensics firm secured the servers and no contact was made with the attackers.
- **Potential Compromised Information:** The potential information includes information related to employment, including: First and last names, SSNs, addresses, driver's license numbers, account information, and information related to health insurance.
- **Any steps the business has taken or plans to take relating to the breach of the security of a system**: MSG has enhanced security measures by requiring Multi-Factor Authentication ("MFA") for all Microsoft 365 services and VPN access. Remote Desktop Services ("RDS") access has been restricted, so users must now connect through their VPN with MFA. Additionally, service account passwords have been strengthened for increased complexity. They have implemented Extended Detection and Response ("XDR") and Managed Detection and Response ("MDR") solutions, ensuring their systems are monitored 24/7 with immediate response to any issues. Furthermore, they have conducted a comprehensive audit of all firewall rules.

Please let me know if more information is needed. Thank you kindly,
Christine

Christine A. Chasse RN, JD, MSN, CIPP/US | Associate Attorney
Spencer Fane LLP

5700 Granite Parkway, Suite 650 | Plano, TX 75024
O 214.459.5884 **M** 817.773.8165
cchasse@spencerfane.com | spencerfane.com

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/customending

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>

<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are contacting you regarding a data security incident that we believe occurred on or about July 29, 2024 when an unauthorized user accessed a Martin Sprocket & Gear, Inc. ("MSG") server storing various types of employee data. As a result of this security incident, some of your personal information may have been exposed to others. Out of an abundance of caution, we are notifying you of this incident.

What Happened

On or about August 22, 2024, we became aware that an unauthorized user accessed our server. We quickly obtained a reputable third-party forensics provider to analyze the scope of the unauthorized access. We are cooperating with law enforcement in its investigation. On November 19, 2024, after learning more information through the investigation into this security incident, MSG became aware that certain personally identifiable information was contained within the server. We are notifying you of this incident at this time.

What Information Was Involved

Although the specific information that was contained within the server varies by individual, such information may include employment information such as: first and last name, date of birth, health information associated with insurance plan coverage, driver's license, financial account and payment card information, and/or Social Security number.

What We Are Doing

At MSG, we take the responsibility of maintaining non-public information seriously. We have, and will continue to, implement additional security controls to reduce the risk of a similar incident occurring again. In addition, we are offering identity theft protection services to all impacted adults through IDX, a ZeroFox Company, data breach and recovery services experts. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. You will be able to contact a Call Center to ask any questions you may have about your identity theft monitoring service.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling [TFN], going to https://response.idx.us/customending, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is [Enrollment Deadline].

Again, at this time, we are not aware of any additional evidence indicating that your information has been used for fraudulent purposes. However, we encourage you to take full advantage of this service offering.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

We deeply regret that this has occurred and apologize for any inconvenience or concern caused by this incident. Please call [TFN] if you'd like to speak to someone. Alternatively, you may go to https://response.idx.us/customending for assistance or for any additional questions you may have.

Sincerely,

Chuck Reynolds

Chuck Reynolds
Chief Business Executive
Martin Sprocket & Gear, Inc.

(Enclosure)

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Scan the QR image or go to https://response.idx.us/customending and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at [TFN] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

North Carolina Residents: Visit the North Carolina Attorney General's Office Consumer Protection Division site (www.ncdoj.gov) for additional information on protection against identity theft. You may also reach them at 919-716-6000 or toll-free within North Carolina at 877-566-7226. Their mailing address is 9001 Mail Service Center, Raleigh, NC 27699-9001.

Maryland Residents: Visit the Maryland Attorney General's website (https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/businessGL.aspx) to learn more about the Personal Information Protection Act. You may also reach them at their roll-free number 1-888-743-0023. Their mailing address is 200 St. Paul Place, Baltimore, MD 21202.

Texas Residents: Visit the Texas Consumer Protection website (https://oag.my.salesforce-sites.com/CPDOnlineForm) for additional information on protection against identity theft. Office of the Attorney General of Texas, PO Box 12548, Austin, TX 78711-2548.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.