Roland Machinery Company

816 North Dirksen Parkway
Springfield, Illinois 62702

<u>NOTICE OF DATA BREACH</u>

July 8, 2026

Dear Valued Customer:

We are writing to notify you of a recent cybersecurity incident that may have involved information your organization previously provided as part of a transaction or credit application. We take the protection of personal information very seriously and are sending this correspondence to inform you of what happened, what information may be involved, what we have done, and what you can do to address this situation.

<u>What Happened</u>

Roland Machinery (Roland) recently identified unauthorized activity by a third party within an isolated portion of Roland's on-premises technology environment. The ongoing investigation determined that an unauthorized actor had access to certain systems on May 28 and May 29, 2026. On June 9, 2026 we were able to confirm that data was removed from a single device. We have not seen any additional unauthorized activity in Roland's system since we began our investigation.

<u>What Information Was Involved</u>

Though our investigation has not determined with certainty which specific files or records were accessed, files may contain personal information provided as part of a purchase and/or credit application. Depending upon how your company is structured and what information may have been provided, an individual's personal information may be included in those files. Any personal information obtained by the unauthorized third party may include name(s), contact information, social security number(s) and/or financial account information that was provided.

<u>What We Are Doing</u>

Upon discovery, we immediately initiated our incident response procedures, secured the affected systems, engaged independent cybersecurity specialists to conduct a forensic investigation, and notified law enforcement, where appropriate. This notice has not been delayed due to law enforcement investigation. We have additionally taken a number of technical and administrative steps to further enhance the security of our systems and customer data.

What You Can Do

Review the type of information your company provides as part of a credit application to understand if any individual's personal information may have been included in a credit application to Roland.

As described in the enclosed document titled "Additional Resources," we recommend you remain vigilant and take steps to protect against potential identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for signs of suspicious activity.

To further protect your personal identity, you may report any suspected incident of identity theft to local law enforcement or state's Attorney General. As a further precaution, we are also providing the option for potentially impacted individuals to access credit monitoring at no charge. These services provide alerts for up to twelve (12) months from date of enrollment when changes occur to your credit file. Such notification is typically sent to you the same day any change or update takes place with the bureau. To enroll in Credit Monitoring services at no charge, please contact IDX by logging onto https://app.idx.us/account-creation/protect and following instructions provided. When prompted please provide the following unique code to receive services: GG6LIX0NV

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and an email account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Roland is not aware of any other exposure that resulted from this incident, however we recommend being mindful of phishing attempts such as emails from unknown senders or those that contain unusual content, such as links or attachments, or being asked to provide personal information over the phone. It is good practice to independently verify any source asking you for your information.

For More Information

We apologize for any concern or inconvenience this incident may cause. We are fully committed to protecting your information and deeply regret that this incident occurred. If you have questions or concerns regarding this incident, please contact (888) 201-1633 Monday through Friday from 8:00 am to 5:00pm CST, excluding Holidays.

Sincerely,

Roland Machinery

ADDITIONAL RESOURCES

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report from www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies (see the "Important Contacts" section for contact details).

You should remain vigilant for incidents of fraud or identity theft by reviewing account statements and monitoring free credit reports. When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. You should also call your local police department and file a report of identity theft. Finally, you should make sure to keep a copy of the police report in case you need to provide it to creditors or credit reporting agencies when accessing or disputing inaccurate information.

You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information about you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies (see the “Important Contacts” section for contact details).

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- Full name, with middle initial and any suffixes;
- Social Security number;
- Date of birth (month, day, and year);
- Current address and previous address for the past five (5) years;
- Proof of current address, such as current utility bill or telephone bill;
- Other personal information as required by the applicable credit reporting agency.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. Initial fraud alerts last one year and are placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the credit reporting agencies listed below. The agency you contact will then contact the other two credit agencies.

Important Contacts

To access your credit report, or to implement a security freeze or a fraud alert, you may contact three major credit reporting agencies listed below.

	Access your Credit Report	Implement a Security/Credit Freeze	Implement a Fraud Alert
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit-reportservices	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-reportservices/credit-fraud-alerts
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/fraud/center.html
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze	P.O. Box 2000 Chester, PA 19016-2000 1-800-680-7289 www.transunion.com/fraud-alerts

For more information about fraud alerts, security freezes, and steps for avoiding identity theft, or if you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you can contact the Federal Trade Commission (FTC) at: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, by phone at 1-877-438-4338, or by visiting www.consumer.ftc.gov. You should also report incidents of suspected identity theft to local law enforcement and the Attorney General's Office in your home state and file a police report.

- District of Columbia residents may contact the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, https://oag.dc.gov, or by phone at (202) 442-9828 (consumer protection hotline).
- Iowa and Oregon residents are advised to report any suspected identity theft to law enforcement, to their respective Attorney General, and to the FTC.
- If you are a Maryland resident, you may contact the Maryland Office of the Attorney General, Consumer Protection Division Office, at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023, or 410-528-8662, or at https://marylandattorneygeneral.gov/pages/contactus.aspx.
- North Carolina residents may contact the North Carolina Office of the Attorney General, Consumer Protection Division, at 9001 Mail Service Center, Raleigh, NC 21699-9001, www.ncdoj.gov, or by phone at 1-877-566-7226.
- Rhode Island residents may contact the Office of the Attorney General at 150 South Main Street, Providence, RI 02930, or by phone (401-274-4400).
- Massachusetts residents are advised of their right to obtain a police report in connection with this incident.
- New York residents, in addition to considering placing a security freeze on their credit reports, may report any incidents of suspected identity theft to law enforcement, including the FTC, the New York Attorney General, or local law enforcement. More information is available at the New York Department of State Division of Consumer Protection website, https://dos.ny.gov/consumer-protection, the NY Attorney General at https://ag.ny.gov or by phone at 1-800-771-7755; or via the FTC at www.ftc.gov/bcp/edu/microsites/idtheft or https://www.identitytheft.gov/#/.