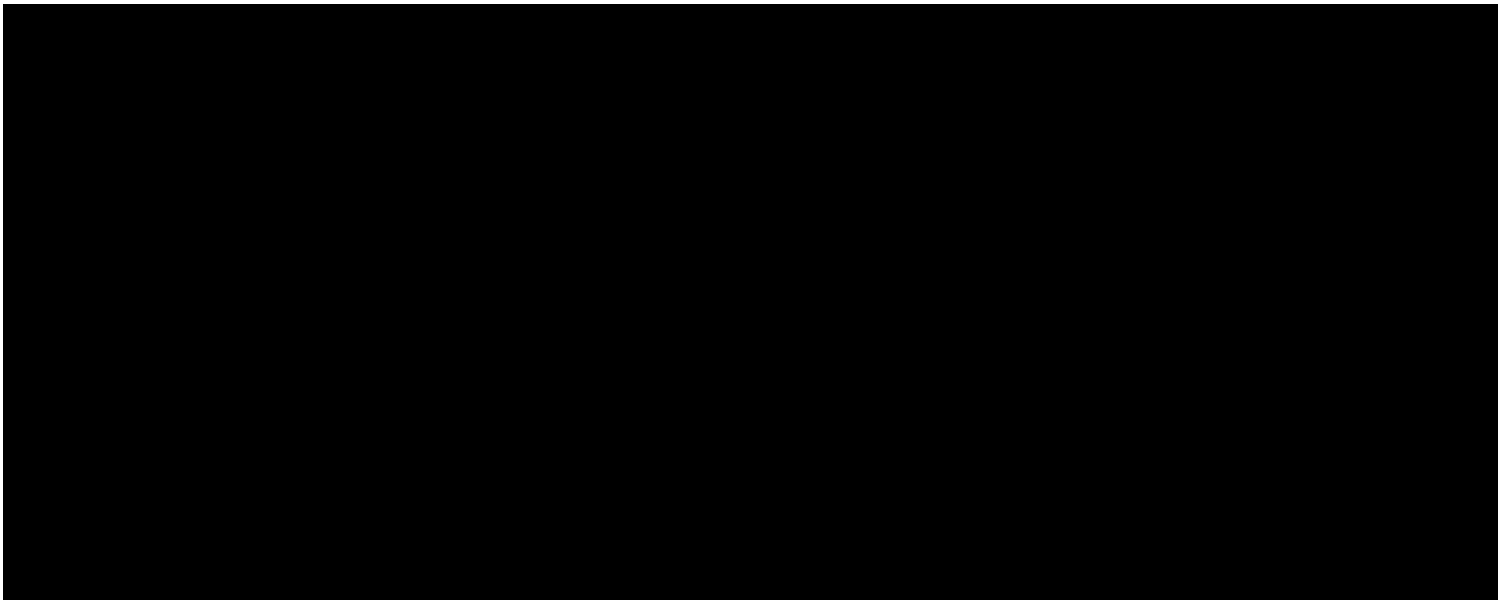




To the Office of the Maryland Attorney General:

Pursuant to Md. Code Com. Law, Title 14, § 14-3504, Messer Cutting Systems, Inc., W141 N9427 Fountain Blvd., Menomonee Falls, WI 53051 (“Messer”), through its attorneys Michael Best & Friedrich, LLP, Attn. Attorney Elizabeth A. Rogers, 620 Congress Ave., Ste. 200, Austin, TX 78701 (“MBF”), is writing to provide this notice of a security breach that unknown and unauthorized threat actors gained access to its network and servers that may have resulted in the unauthorized acquisition of personal information.

Messer believes that three (3) Maryland residents were impacted by this breach.

On Monday, December 26, 2022, Messer, determined that unknown and unauthorized threat actors gained access to its network and servers. Immediately upon detecting the unauthorized access, Messer engaged the services of an outside law firm to provide legal advice and direction in support of the incident response. The law firm hired a vendor to help Messer investigate the activities of the unauthorized threat actors. After a detailed review, Messer, in collaboration with outside counsel, determined on January 5, 2023, that some of the files contained personal data and that those files were accessed by the unknown and unauthorized threat actors.

The personal information that an unauthorized threat actor may have accessed includes your first and last name, address, date of birth, Social Security number, Driver’s License number, state ID number, and telephone number.

We have engaged third party cybersecurity experts to respond to and investigate this incident, as well as restore and secure our systems to determine what information was impacted. In addition, we have enhanced the security of our systems and have installed industry leading advanced endpoint threat detection and mitigation tools.

There was no delay in providing you this notification as a result of law enforcement investigation.

Attached is a copy of the notification letter that Messer will place in the U.S. Mail Thursday, January 26, 2023 to the affected individuals. Please let us know if you have any questions or would like to discuss further.

Sincerely,

Elizabeth A. Rogers, CIPP/US

Partner

T 512.640.3164 | M 512.924.7977

earogers@michaelbest.com | [bio](#)



Email Disclaimer

The information contained in this communication may be confidential, is intended only for the use of the recipient(s) named above, and may be legally privileged. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please return it to the sender immediately and delete the original message and any copy of it from your computer system. If you have any questions concerning this message, please contact the sender.



Messer Cutting Systems, Inc.
W141 N9427 Fountain Blvd.
Menomonee Falls, WI 53051
Ph. 262.255.5520
www.messer-cs.com

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you about a data security incident that affected the systems of Messer Cutting Systems, Inc. ("Messer"), which may have involved your personal data. We value our relationship with you and take the security of your data seriously. We recommend that you closely review the information provided in this letter for some steps that you may take to help protect yourself against potential misuse of your information.

What Happened

On Monday, December 26, 2022, Messer, determined that unknown and unauthorized threat actors gained access to its network and servers. Immediately upon detecting the unauthorized access, Messer engaged the services of an outside law firm to provide legal advice and direction in support of the incident response. The law firm hired a vendor to help Messer investigate the activities of the unauthorized threat actors. After a detailed review, Messer, in collaboration with outside counsel, determined on January 5, 2023, that some of the files contained personal data and that those files were accessed by the unknown and unauthorized threat actors. The investigation is ongoing.

There was no delay in providing you this notification as a result of law enforcement investigation.

What Information Was Involved

The personal information that an unauthorized threat actor may have accessed includes your first and last name, address, date of birth, Social Security number, Driver's License number, state ID number, and telephone number.

Here's What We Are Doing

We have engaged third party cybersecurity experts to respond to and investigate this incident, as well as restore and secure our systems to determine what information was impacted. In addition, we have enhanced the security of our systems and have installed industry leading advanced endpoint threat detection and mitigation tools.

Additionally, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 24-months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. It is recommended that you remain vigilant for incidents of fraud and identity theft and report suspected incidents of identity theft to local

law enforcement or the attorney general. We recommend that you carefully monitor your free credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. You should also regularly review your credit or debit card account statements to determine if there are any discrepancies or unusual activity listed. If you see something you do not recognize, immediately notify your financial institution.

For More Information

If you have any further questions or concerns regarding this matter, please contact (855) 624-6817, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

A handwritten signature in black ink, appearing to read "Scott", with a long horizontal flourish extending to the right.

Scott C. Kessler
President and CEO - Americas

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

**TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.