

CONFIDENTIAL TREATMENT REQUESTED

December 29, 2024

BY EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Mayer Brown LLP
1999 K Street, N.W.
Washington, DC 20006-1101
United States of America

T: +1 202 263 3000
F: +1 202 263 3300
mayerbrown.com

Amber Thomson
Partner
T: (202) 263-3456
athomson@mayerbrown.com

RE: Medical Technology Industries Inc. –
Notification of Incident

To Whom It May Concern:

In accordance with Maryland's Personal Information Protection Act (PIPA), Md. Code Ann. Comm. Law 14-3504, we write on behalf of our client, Medical Technology Industries Inc. ("MTI") to inform you of a cybersecurity incident.

MTI designs, manufactures, and provides specialized medical and dental exam room equipment to specialty physicians. On December 6, 2024, MTI learned that a criminal ransomware group gained unauthorized access to certain systems within MTI's network and potentially exfiltrated certain MTI data. MTI promptly launched an investigation, engaging cybersecurity experts to assist in assessing the scope of the incident and taking steps to mitigate any potential impact and contain the incident. During the course of the investigation, there has been engagement with law enforcement, including the Federal Bureau of Investigation.

MTI's investigation has determined that certain company data may have been acquired by an unauthorized third party as part of a data breach. The types of information that may have been impacted includes one or more of the following: name, Social Security number, and date of birth.

To date, there are 4 Maryland residents whose personal information was subject to the breach. These individuals will be sent a notification letter on December 30, 2024.

MTI is committed to the protection of personal information in its care and takes this responsibility seriously. The company is working to further enhance its security measures, including with respect to further restricting external access to its network.

Should you have any questions or require further information, please do not hesitate to contact me.

Mayer Brown LLP

Office of the Attorney General
December 29, 2024
Page 2

**CONFIDENTIAL TREATMENT
REQUESTED**

Sincerely,

A handwritten signature in black ink, appearing to read "Amber Thomson". The signature is fluid and cursive, with the first name "Amber" and last name "Thomson" clearly distinguishable.

Amber Thomson
Partner

Enclosures: Consumer Notification Letter



<<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>> <<last_name>>,

Medical Technology Industries, Inc. (“MTI”) is writing to inform you of a cybersecurity incident that may have impacted your personal information. We are contacting you to explain the circumstances of the incident, the types of information involved, and protective measures you can take, should you deem it appropriate to do so.

What happened?

On December 6, 2024, MTI learned that an unauthorized third party gained access to certain systems within MTI’s network. We promptly terminated the unauthorized access to the affected systems, launched an investigation, notified law enforcement, and engaged leading cybersecurity vendors to help assess the scope of the incident. MTI has since determined that certain individuals’ personal information may have been acquired by an unauthorized third party.

What information was involved?

Our investigation determined that the following types of your personal information may have been impacted: your name, Social Security Number, and date of birth.

What we are doing.

MTI takes this incident and the security of information in our care seriously. We are working with leading cybersecurity firms to support our investigation and further enhance our security measures, including implementing heightened monitoring and additional information security safeguards.

What you can do.

To help relieve concerns and restore confidence following this incident, we are offering complimentary access to Kroll’s Identity Monitoring Services 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 deadline)>> 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 or refer to the details in the enclosed “Additional Resources”.

In addition to activating the identity monitoring, we recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please review the enclosed “Additional Resources” for additional guidance.

For more information.

We take the privacy and security of your information very seriously. We sincerely regret any worry or inconvenience this matter may cause you. If you have further questions or concerns about this incident, please call us at 801-875-4940.

Sincerely,

A handwritten signature in black ink, appearing to read "Rudy H. Bak". The signature is fluid and cursive, with a long horizontal stroke at the end.

President, MTI

Sample

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 online at 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, 303485281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

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

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.

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 listed below.

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com/personal/credit-report-services, 1-800-685-1111

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

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

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:

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

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts. You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is 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 the 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 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed above. The agency you contact will then contact the other two credit agencies.

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, <https://www.marylandattorneygeneral.gov/>, 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/>. The NYS Department of State's Division of Consumer Protection may be contacted at (800) 697-1220 or <https://www.dos.ny.gov/consumerprotection>.

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

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

KROLL

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.