UMS®
UNITED MEDICAL SYSTEMS

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

KROLL
SCAN TO ENROLL

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

Dear <<First_name>> <<Last_name>>,

United Medical Systems (DE), Inc. ("UMS") writes to inform you of a data event that may affect certain information related to you. Please note, Massachusetts law restricts the information UMS is permitted to include in this letter. However, we take this matter seriously and write to provide you with the information we are able to provide, as well as information regarding resources we are making available to you.

The categories of information identified in the review of relevant information include your <<b2b_text_2 (name, data elements)>>.

The obligation to safeguard the information in our care is of paramount importance to UMS. UMS immediately responded to the suspicious activity and engaged specialists to conduct a comprehensive and diligent investigation. Once all necessary information was confirmed, UMS notified relevant individuals and requisite regulatory authorities. Moreover, in response to this event, we have also taken steps to further enhance our existing cybersecurity infrastructure, as well as implement additional policies and procedures to minimize the reoccurrence of a future similar event.

Although we have no evidence that your information was misused in connection with this matter, out of an abundance of caution, we are offering you access to twenty-four (24) months of identity monitoring services through Kroll, at no cost to you. Please understand that due to privacy laws, UMS is not able to activate these services for you directly. Additional information regarding how to activate the complimentary monitoring service is in the "*Steps You Can Take to Help Protect Your Information*" section of the letter below.

In addition to enrolling in the complimentary monitoring services we are offering you, we recommend that you remain vigilant against incidents of fraud and identity theft by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. If you discover suspicious or unusual activity on your account(s), it is recommended that you promptly contact your financial institution or credit/debit card company. You can also review the enclosed "*Steps You Can Take to Help Protect Your Information*" for additional information and resources.

We understand you may have additional questions about this matter. Should you have questions or concerns regarding this matter or the offered monitoring services, please contact our dedicated assistance line through Kroll at [redacted], which is available Monday to Friday between the hours of 9:00 a.m. – 6:30 p.m. Eastern Time, excluding some U.S. holidays.

Sincerely,

United Medical Systems (DE), Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Offered Monitoring Services

As an added measure, we are providing complimentary access to the following monitoring 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. 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.

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.

To enroll in the offered services, please take the following steps:

- Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
- *Please note, 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 the monitoring services, please visit info.krollmonitoring.com.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and

7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com	**Experian** 1-888-397-3742 www.experian.com	**Equifax** 1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	**Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013	**Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	**Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.