CERAPEDICS
Enhancing the Science of Bone Repair

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

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

Re: Notice of Data Breach

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

We are writing to inform you of a data security incident experienced by Cerapedics, Inc. ("Cerapedics") that may have affected your personal information. Cerapedics is a medical device manufacturer which develops bone graft substitute used in orthopedic surgeries. At Cerapedics, we take the privacy and security of personal information very seriously. This letter contains information about the incident and steps you can take to help protect your personal information.

What Happened? On or about August 4, 2020, Cerapedics discovered unusual activity within its email system. Upon discovering this activity, Cerapedics took immediate steps to secure its digital environment and began an investigation. In so doing, Cerapedics engaged an independent cyber forensics firm to determine what happened and whether any personal information was affected. On August 18, 2020, Cerapedics learned that it was the victim of a cybersecurity incident whereby an unauthorized actor gained access to a Cerapedics employee email account. After learning this information, Cerapedics continued to work with the cyber forensics firm from August through November of 2020 to confirm that the scope of access was limited to one account, and to review the account to determine the extent of information contained therein. On November 22, 2020, Cerapedics learned that messages and attachments contained within the accessed email account included some of your personal information. Cerapedics is therefore providing you notification and information about steps you can take to help protect your personal information.

Please note that this unauthorized access was limited to information transmitted via email only; there was no unauthorized access to any other information systems.

What Information Was Involved? The following information may have been involved in the incident: your name and address, Social Security number, driver's license number/state identification number, financial account information, payment card information, medical information, online credentials, and/or digital signature.

What We Are Doing. As soon as Cerapedics discovered the incident, we took the steps described above. We have also implemented additional security features within our email system to reduce the risk of similar incidents occurring in the future.

In addition, we have arranged for you to activate, at no cost to you, in an online identity monitoring service for one year provided by Kroll. Your identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **March 23, 2021** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

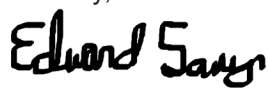
Additional information describing your services is included with this letter.

What You Can Do. We encourage you to follow the recommendations included on the following page and activate the complimentary identity monitoring services we are offering.

For more information: Further information about how to protect your personal information appears on the following page. If you have questions, please call 1-833-971-3286, Monday through Friday from 7:00 a.m. – 4:30 p.m. Mountain Standard Time, excluding major U.S. holidays.

We apologize for any worry or inconvenience that this incident may cause you.

Sincerely,



Edward Sawyer
General Manager
Cerapedics, Inc.

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-800-916-8800	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. A security freeze may be placed or lifted free of charge. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Protecting personal information of a Minor: You can contact the three national credit reporting agencies to request a search for a credit report associated with a minor's Social Security number. If a report exists, request a copy and immediately report fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at https://www.identitytheft.gov/. For more information visit: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.

Kroll | A Division of DUFF&PHELPS

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 will 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.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.