[redacted]

August 18, 2016

Dear [redacted],

DXE Medical, Inc. values the relationship we have with our customers and understands the importance of protecting personal information. We are writing to notify you of an incident that may involve your payment card information.

On July 28, 2016, we were advised by our third-party website developer that it had identified code it did not recognize on the server that operates our e-commerce website. We immediately began an investigation, removed the code, and determined that the code was designed to copy data that was entered by customers during the checkout process. According to the investigation, if a customer attempted to or did place an order on AED.com from March 24, 2016 to July 29, 2016, information associated with the order being placed, including the customer's name, address, payment card number, expiration date and card verification code, may have been obtained by an unauthorized third-party. We are notifying you because you used a payment card ending in [redacted] on our website during the affected time period.

To date, we have not received any reports from customers of misuse of their card. However, we advise you to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take to protect your information.

We are notifying the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring on the affected cards. We also continue to work further to strengthen the security of our systems to help prevent this from happening in the future.

We regret any inconvenience or concern this may have caused. If you have questions, please call (866) 349-4363 from 9 a.m. to 6 p.m. EST, Monday through Friday.

Reuben Dickenson
General Manager

## MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
*Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
*TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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