<<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>>

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

NOTICE OF DATA BREACH

Dear <<first_name>> <<last_name>>:

Boston Scientific Corporation ("Boston Scientific") is committed to protecting the privacy and security of the personal data entrusted to us. We want to provide you with information about a recent cybersecurity incident that affected certain personal information. Following a detailed investigation and comprehensive data review, on November 05, 2026, we determined that some of your personal information was included.

We are sharing the following information about what happened, what information was involved, the actions we have taken and resources available to assist you.

What Happened?

Boston Scientific became aware of potential unauthorized access to company data on May 12, 2026. In response, we promptly activated our cybersecurity incident response protocols and began an investigation with the assistance of third-party cybersecurity experts.

Our investigation determined that the unauthorized parties gained access to certain cloud-based IT business applications through social engineering (vishing) tactics and downloaded data between May 7 and May 12, 2026. Social engineering is a growing trend of cyberattacks across the globe that includes tricking individuals into providing their log-in credentials, such as calling and pretending to be a customer or member of the IT department.

Our operations, manufacturing, ordering, and distribution processes were not disrupted and our ability to serve patients and healthcare providers was not affected by this incident. There also was no impact to the operation, performance, remote monitoring or safety of Boston Scientific products or medical devices.

What Personal Information Was Involved?

Your personal information involved in this incident included the following: <<b2b_text_1 (DataElements)>>. Your Social Security Number and financial information were not affected.

The information did not include data from remote monitoring systems (such as the LATITUDE Patient Management System), connected medical devices, clinical case management or workflow applications or patient medical record systems.

What We Are Doing

We took prompt action to contain and investigate the incident, identify the affected systems and data, and notify and cooperate with law enforcement.

We also continue to take appropriate and proactive steps to further strengthen our security infrastructure. This includes enhanced monitoring and detection, strengthened access controls and additional cybersecurity awareness training for our teams.

What You Can Do

While we are not aware of fraud or misuse of your personal information associated with this incident, as a general precaution, we encourage individuals to remain vigilant against identity theft and fraud. This includes using unique passwords and keeping them confidential, paying close attention to communications requesting personal data or that urge immediate action, reviewing account statements, and promptly reporting suspicious activity.

For More Information

Again, we take the protection of your personal information seriously and sincerely regret the concern this notice may cause. If you have additional questions, please contact our dedicated assistance line at (844) 301-0384, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Boston Scientific

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be 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, 1-888-378-4329
- *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

Fraud Alerts: There are two types of general 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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Boston Scientific's mailing address is 300 Boston Scientific Way, Marlborough, MA 01752-1234 and its phone number is 1 (888) 272-1001.