

May 23, 2024

Via E-mail (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

In accordance with Md. Code Ann., Com. Law § 14-3504, I am writing on behalf of LivaNova USA, Inc. (“LivaNova” or the “Company”) to notify you regarding the nature and circumstances of a data security issue.

On November 19, 2023, the Company detected a cybersecurity incident that resulted in a disruption to portions of its information technology systems. Promptly after detecting the issue, the Company began an investigation with assistance from external cybersecurity experts and coordinated with U.S. law enforcement. The Company took actions to remediate the issue, such as taking certain systems offline.

Based on its investigation, the Company determined that the issue was attributable to the zero-day Citrix Bleed vulnerability. The incident involved the deployment of ransomware by a threat actor group believed to be LockBit 3.0. The threat actor used the Citrix Bleed vulnerability to gain access to LivaNova’s network, exfiltrate certain Company data and deploy ransomware. The threat actor demanded payment in exchange for a decryption key. The Company chose not to pay the ransom demand. The Company instead worked diligently to rebuild and restore the affected systems and data. The threat actor published the exfiltrated data on its dark web TOR site, which was taken down by international law enforcement authorities on February 20, 2024.

The Company determined on May 13, 2024 that certain personal information of one (1) Maryland resident was affected by the incident. The affected information of the Maryland resident included name, Social Security number, date of birth and employee ID. LivaNova is notifying the affected Maryland resident and offering him two years of complimentary credit monitoring and identity protection services.

Office of the Attorney General

May 23, 2024

Page 2

Attached for your reference is a copy of the notice being sent to the affected individual.
Please do not hesitate to contact me if you have any questions.

Very truly yours,

A handwritten signature in black ink that reads "Lisa J. Sotto". The signature is written in a cursive, flowing style.

Lisa J. Sotto

Enclosure

[Insert], 2024

[Insert address]

NOTICE OF DATA BREACH

Dear Colleague,

We are writing to notify you of a cybersecurity incident that involves certain of your personal information.

What Happened?

As you are aware, LivaNova was affected by a cybersecurity incident that occurred around October 26, 2023, which we identified on November 19, 2023. The incident affected some of our information technology systems and certain personal information of some current and former employees and contingent workers. We regret that this matter affected certain of your personal information.

What Information Was Involved?

The types of personal information affected varied by individual and included information such as name, contact information (e.g., telephone number, email and postal address), Social Security number, date of birth, financial account information (e.g., bank account data), health insurance information, online credentials, and work-related information (e.g., employee ID, compensation, disability status and evaluations).

What We Are Doing

Promptly after detecting the issue, we began an investigation with assistance from external cybersecurity experts and coordinated with law enforcement. We also quickly took steps to protect our systems and data, and to mitigate the impact of the incident, including shutting down certain systems and requiring personnel to change their passwords. We take the protection of personal information very seriously and continue to enhance our security safeguards.

What You Can Do

Although we currently do not have evidence of harm to individuals resulting from this issue, we are alerting you so you can take steps to help protect your personal information. We recommend that you remain vigilant for incidents of fraud and identity theft by staying alert for unsolicited communications involving your personal information, reviewing your account statements for suspicious activity and monitoring your free credit reports.

To further assist you, LivaNova is offering you two years of free identity protection and credit monitoring services through Experian IdentityWorks. These services are available to you for two years from the date of enrollment and require action on your part. To enroll in these services:

1. Ensure that you enroll by **August 30, 2024**
2. Visit the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/credit>
3. Provide your activation code: [REDACTED]

Additional information, terms of these services, self-help tips and information about identity protection are located at <https://www.experianidworks.com/credit>.

More Information

We regret any inconvenience this issue may cause you. If you have questions about this issue or the Experian IdentityWorks services, or if you would like an alternative to enrolling in the services online, please contact Experian's customer care team toll-free at 833-931-5100, Monday through Friday 8 a.m. to 8 p.m. CT (excluding major U.S. holidays). Please reference engagement number B119941 when calling.

Sincerely,



Vladimir Makatsaria
Chief Executive Officer

U.S. Reference Guide

We encourage affected individuals to take the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit <https://www.identitytheft.gov>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime. You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.marylandattorneygeneral.gov

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act (“FCRA”). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General’s Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General’s Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)-274-4400
<http://www.riag.ri.gov>

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.