UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

CRYSTAL SCHULTZ, *individually and on behalf of all others similarly situated*, Plaintiff, v. LIVANOVA, USA, INC., Defendant.	Case No.: 4:24-cv-02276 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Crystal Schultz ("Plaintiff"), individually and on behalf of the Class defined below of similarly situated persons, alleges the following against Defendant, LivaNova USA, Inc. ("LivaNova" or "Defendant"), based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by counsel as to all other matters:

SUMMARY OF THE CASE

1. This action arises from LivaNova's failure to secure the personal identifiable information ("PII")[1] and protected health information ("PHI")[2] (collectively "Private

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R.

Information") of Plaintiff and the members of the proposed Class, where LivaNova designs, develops, manufactures, and sells medical devices to Plaintiff and Class Members.

2. LivaNova is a global medical technology company "built on decades of experience and a relentless commitment to patients" whose "products and therapies are used worldwide."[3]

3. On or about November 19, 2023, LivaNova discovered that an unauthorized party had obtained Plaintiff's and Class Members' Private Information from LivaNova's computer systems (the "Data Breach").[4]

4. The Private Information that intruders accessed and infiltrated from LivaNova's systems included, at the very least name, contact information including phone number, email and postal address, date of birth, medical information, treatment, condition, diagnosis, prescription, physician, medical record number and device serial number, and health insurance information.

5. As a result of the Data Breach, which LivaNova failed to prevent, the Private Information of patients of physicians and healthcare professionals who are LivaNova's clients, including Plaintiff and the proposed Class Members, was stolen.[5]

6. Among myriad industry standards and statutes for protection of sensitive information, PHI is specifically governed by federal law under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations. HIPAA requires

---

§ 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited June 11, 2024).

[3] *About Us*, LIVANOVA, https://www.livanova.com/en-us/about-us (last visited June 11, 2024).

[4] *See* Notice Letter, dated May 31, 2024, attached as **Exhibit A**.

[5] *See id*.

entities like LivaNova to take appropriate technical, physical, and administrative safeguards to secure the privacy of PHI, establishes national standards to protect PHI, and requires timely notice of a breach of unencrypted PHI.

7. Instead, LivaNova disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard its Patients' Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. LivaNova's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

8. Further exacerbating Plaintiff's injuries, LivaNova has offered insufficient assurances that all personal data or copies of data have been recovered or destroyed, or that LivaNova has adequately enhanced its security practices or dedicated sufficient resources and staff to avoid a similar breach of its network in the future.

9. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and uncompensated time spent responding to and remedying the effects of the Data Breach; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) expense and time spent on initiating fraud alerts and contacting third parties; (k) decreased credit scores; (l) lost work time; (m) anxiety, annoyance, and nuisance; (n) continued risk to their Private Information, which remains in LivaNova's

possession and is subject to further breaches so long as LivaNova fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information; and (o) disgorgement damages associated with LivaNova's maintenance and use of Plaintiff's data for its benefit and profit..

10. Plaintiff and Class Members would not have provided their valuable PII and sensitive PHI had they known that LivaNova would make their Private Information Internet-accessible, not encrypt personal and sensitive data elements and not delete the Private Information it no longer had reason to maintain.

11. Through this lawsuit, Plaintiff seek to hold LivaNova responsible for the injuries it inflicted on Plaintiff and Class Members due to its impermissibly inadequate data security measures, and to seek injunctive relief to ensure the implementation of security measures to protect the Private Information that remains in LivaNova's possession.

JURISDICTION AND VENUE

12. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of Class Members is about 180,000 people, many of whom have different citizenship from LivaNova. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A). Plaintiff is a citizen of New York. Defendant is a citizen of Texas.

13. This Court has personal jurisdiction over Defendant because the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from the Houston Division of the Southern District of Texas. Defendant has its principal place of business located in the Houston

Division of the Southern District of Texas, sufficient contacts in Texas, as it conducts a significant amount of its business in the state of Texas.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) because it is in the Houston Division of the Southern District of Texas in which a substantial part of the events or omissions giving rise to the claim occurred.

PARTIES

15. Plaintiff Crystal Schultz is, and at all relevant times has been, a resident and citizen of East Rochester, NY, where she intends to remain.

16. Defendant LivaNova is a Delaware corporation with its principal place of business located at 100 Cyberonics Blvd Ste 600, Houston, Texas 77058. The registered agent for service of process is Universal Registered Agents, Inc., 7533 County Road 1127, Godley, Texas 76044.

FACTUAL ALLEGATIONS

A. The LivaNova Data Breach

17. LivaNova provides medical technology software to customers to "[transform] lives with products and therapies for the head and heart."[6]

18. To obtain medical products, customers, including Plaintiff and Class Members, were required to provide sensitive and confidential Private Information, including their names, dates of birth, address, health records, insurance information, and other sensitive information, that would be held by Defendant in its computer systems.

19. On or about October 26, 2023, Plaintiff's and Class Members' Private Information in possession of LivaNova was obtained by an unauthorized party, which LivaNova describes in

[6] https://www.livanova.com/en-us/about-us (last visited June 11, 2024).

its Notice Letter as "an unauthorized party obtained certain identifiable personal information of U.S. patients" which "resulted in a disruption to portions of our IT systems."[7]

20. Approximately seven months later, on May 31, 2024, LivaNova began sending out Notice Letters to affected persons, informing them that their Private Information had been compromised in the Data Breach[8]

21. The Notice Letter states LivaNova "promptly after detecting the issue, [they] began an investigation with assistance from external cybersecurity experts and coordinated with law enforcement conducted a robust review of the data to identify individuals whose information may have been impacted and worked to obtain addresses and notify individuals as quickly as possible."[9]

The Data Breach

22. On or about May 31, 2024, Defendant began notifying customers of the Data Breach, informing them in an online Cybersecurity Notice:

> **What Happened?**
>
> We are writing to notify you of a cybersecurity incident at LivaNova that occurred around October 26, 2023, which we discovered on November 19, 2023. The incident resulted in a disruption to portions of our IT systems. Promptly after detecting the issue, we began an investigation with assistance from external cybersecurity experts and coordinated with law enforcement. We took action to remediate the issue, such as taking certain systems offline.
>
> **What Information Was Involved?**
>
> Based on our investigation, on April 10, 2024, we learned that an unauthorized party obtained certain of your personal information. The information, which varied by affected individual, included data such as name, contact information (e.g., phone number, email and postal address), date of birth, medical information (e.g., treatment, condition, diagnosis, prescription, physician, medical record number and device serial number), and health insurance information.

[7] Ex. A.

[8] *See id*.

[9] *Id*

What Can Customers Do?

We are alerting you about this issue so you can take steps to help protect your information. You are entitled to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll. free at 1-877-322-8228. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your free credit reports. We also recommend that you remain alert for unsolicited communications involving your personal information.[8]

23. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

24. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class Members, including name, contact information (e.g., phone number, email and postal address), date of birth, medical information (e.g., treatment, condition, diagnosis, prescription, physician, medical record number and device serial number), and health insurance information. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

25. As evidenced by the Data Breach, the Private Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

B. The Value of Private Information

26. In April 2020, ZDNet reported in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize

damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for complaints as revenge against those who refuse to pay."[10]

27. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[11]

28. Stolen Private Information is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

29. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[12]

30. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data

---

[10] https://www.zdnet.com/article/ransomeware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited June 11, 2024).

[11] *See* https://www.cisa.gov/sites/default/files/2023-01-CISA_MSISAC_Ransomware%20Guide_8508C.pdf (last visited June 11, 2024).

[12] *Shining a Light on the Dark Web with Identity Monitoring, IdentityForce*, Dec. 28, 2020, https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited June 11, 2024).

breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[13]

31. The Private Information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Private Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $2009.[14] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[15] Criminals can also purchase access to entire company data breaches.[16]

32. In addition, due to the highly valuable nature of PHI, the FBI has warned healthcare providers that they are likely to be the targets of cyberattacks like the one at issue here.[17]

33. Once Private Information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

---

[13] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, https://www.armor.com/resources/blog/stolen-pii- ramifications- identity-theft-fraud-dark-web/ (last visited June 11, 2024).

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal- data-sold-on-the-dark-web- how-much-it-costs/ (last visited June 11, 2024).

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is- selling-for-on-the-dark-web/ (last visited June 11, 2024).

[16] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous- browsing/in-the- dark/ (last visited June 11, 2024).

[17] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK2 4U20140820.

34. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

35. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

36. Data breaches facilitate identity theft as hackers obtain consumers' Private Information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

37. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use Private Information to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[18] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[19]

38. The market for Private Information has continued unabated to the present, and in 2023 the number of reported data breaches in the United States increased by 78% over 2022,

[18] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao- 07-737.pdf (last visited June 11, 2024).

[19] *Id*.

reaching 3205 data breaches.[20]

39. The exposure of Plaintiff's and Class Members' Private Information to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

C. Healthcare Organizations are Prime Targets for Cyberattacks.

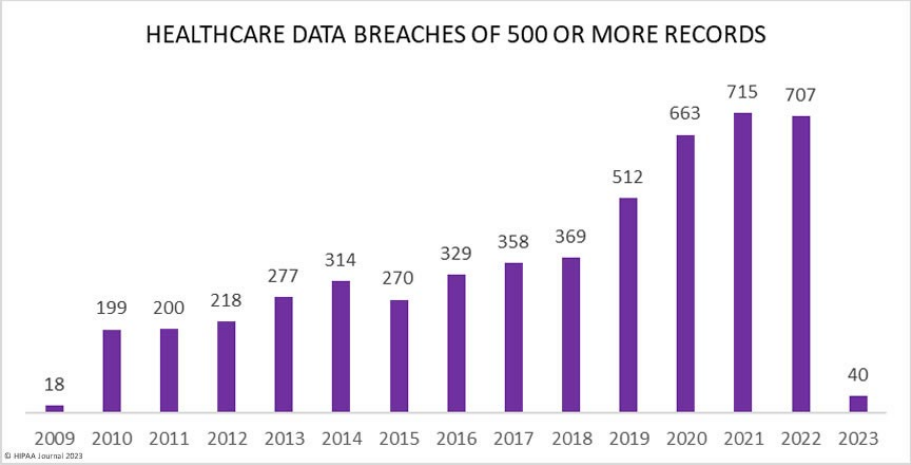
40. Healthcare organizations are prime targets for cyberattacks because of the information they collect and store, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and personal information of employees, customers and patients—all extremely valuable in underground markets.

41. This was known and obvious to LivaNova as they observed frequent public announcements of data breaches affecting the healthcare industry and knew that information of the type it collected, maintained, and stored is highly coveted and a frequent target of cybercriminals.

42. For example, a report by the HIPAA Journal noted that "Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more records have been reported to the HHS' Office for Civil Rights. Those breaches have resulted in the exposure or impermissible disclosure of 382,262,109 healthcare records. That equates to more than 1.2X the population of the United States. In 2018, healthcare data breaches of 500 or more records were being reported at a rate of

[20] Beth Maundrill, *Data Privacy Week: US Data Breaches Surge, 2023 Sees 78% Increase in Compromises*, INFOSECURITY MAGAZINE (Jan. 23, 2024); https://www.infosecurity-magazine.com/news/us-data-breaches-surge-2023/ (last visited June 11, 2024); *see also* Identity Theft Resource Center, *2023 Data Breach Report*, https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited June 11, 2024).

around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[21]



43. Ransomware attacks are especially prevalent in the industry. For years federal agencies have warned about the increasing risk of ransomware attacks on companies holding PII and PHI. For example, in October 2019 the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[22]

44. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to

[21] https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited June 11, 2024).

[22] https://www.ic3.gov/Media/Y2019/PSA191002 (last visited June 11, 2024).

release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[23]

45. In March 2021, Tenable Security Response Team conducted a root cause analysis of 293 healthcare breaches known to have exposed records between January 2020 and February 2021, and concluded that "ransomware was by far the most prominent root case of healthcare breaches, accounting for a whopping 54.95%."[24]

46. At all relevant times, LivaNova knew, or reasonably should have known, of the importance of safeguarding Private Information and the foreseeable consequences that would occur if its data security systems were breached, including, specifically, the significant costs that would be imposed on affected individuals as a result of the breach.

47. LivaNova was, or should have been, fully aware of the significant number of individuals whose Private Information it collected and stored, thus, the significant number of individuals who would be harmed by a breach of LivaNova's systems.

48. Despite all the publicly available knowledge of the serious threat of compromises of personal information and despite holding the Private Information of millions of individuals, LivaNova failed to use reasonable care in maintaining the privacy and security of Plaintiff's and Class Members' Private Information. Had LivaNova implemented adequate security measures, cybercriminals never could have accessed millions of individuals' files and the Data Breach would have been prevented or much smaller in scope.

D. LivaNova Failed to Comply with Regulatory Requirements and Standards.

[23] https://www.cisa.gov/stopransomware/ransomware-faqs#:~:text=Malicious%20actors%20continue%20to%20adjust,as%20secondary%20forms%20of%20extortion (last visited June 11, 2024).

[24] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last visited June 11, 2024).

49. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and the healthcare sector. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

50. For example, at least 24 states have enacted laws addressing data security practices that require businesses that own, license, or maintain Private Information about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access.

51. Additionally, cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting of physical security systems; protecting against any possible communication system; and training staff regarding critical points.[25]

52. The FTC has issued several guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be considered for all business decision-making.[26]

53. Under the FTC's 2016 *Protecting Personal Information: Guide for Business* publication, the FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on

[25] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security (last visited June 11, 2024).

[26] *Start With Security*, Fed. Trade Comm'n ("FTC"), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 11, 2024).

computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[27]

54. The guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

55. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[28]

56. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

57. LivaNova's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

---

[27] *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 11, 2024).

[28] *Supra* n.39.

58. LivaNova's failure to verify that it had implemented reasonable security measures constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

59. Furthermore, LivaNova is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. The Privacy Rule and the Security Rule set nationwide standards for protecting health information, including health information stored electronically.

60. The Security Rule requires LivaNova to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.[29]

61. Pursuant to HIPAA's mandate that LivaNova follow "applicable standards, implementation specifications, and requirements . . . with respect to electronic protected health information," 45 C.F.R. § 164.302, LivaNova was required to, at minimum, "review and modify the security measures implemented . . . as needed to continue provision of reasonable and

[29] *Summary of the HIPAA Security Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited June 11, 2024).

appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(e), and "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

62. LivaNova is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

63. Both HIPAA and HITECH obligate LivaNova to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive customers Private Information. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. § 17902.

64. As alleged in this Complaint, LivaNova has failed to comply with HIPAA and HITECH. It has failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach and loss of data, and failed to ensure the confidentiality and protection of PHI.

E. LivaNova Failed to Comply with Industry Practices.

65. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes

solutions to defend against those cyber-attacks.[30] All organizations collecting and handling Private Information, such as LivaNova, are strongly encouraged to follow these controls.

66. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[31]

67. Several best practices have been identified that a minimum should be implemented by data management companies like LivaNova, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[32]

68. LivaNova failed to follow these and other industry standards to adequately protect the Private Information of Plaintiff and Class Members.

F. The Data Breach Caused Injury to Class Members and Will Result in Additional Harm Such as Fraud.

69. Without detailed disclosure to the victims of the Data Breach, individuals whose Private Information was compromised by the Data Breach, including Plaintiff and Class Members, were unknowingly and unwittingly exposed to continued misuse and ongoing risk of misuse of

[30] Center for Internet Security, *Critical Security Controls*, at 1 (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited June 11, 2024).

[31] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited June 11, 2024).

[32] *See* Center for Internet Security, *Critical Security Controls* (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited June 11, 2024).

their Private Information for months without being able to take available precautions to prevent imminent harm.

70. The ramifications of LivaNova failure to secure Plaintiff's and Class Members' data are severe.

71. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.

72. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[33] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[34]

73. Identity thieves can use Private Information, such as that of Plaintiff and Class Members, which LivaNova failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

74. As demonstrated herein, these and other instances of fraudulent misuse of the compromised Private Information has already occurred and are likely to continue.

[33] 17 C.F.R. § 248.201 (2013).

[34] *Id*.

75. As a result of LivaNova's delay between the Data Breach in October and the notice of the Data Breach sent to affected persons in May, the risk of fraud for Plaintiff and Class Members increased exponentially.

76. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[35]

77. The 2017 Identity Theft Resource Center survey[36] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by identity theft; and
- 7% reported feeling suicidal.

78. Identity theft can also exact a physical toll on its victims. The same survey reported

[35] *Victims of Identity Theft*, Bureau of Justice Statistics (Sept. 2015) http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited June 11, 2024).

[36] *Id*.

that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[37]

79. There may be a time lag between when harm occurs versus when it is discovered, and also between when private information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[38]

Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

G. Plaintiff and Class Members Suffered Damages.

80. As a direct and proximate result of LivaNova's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have already been harmed by the fraudulent misuse of their Private Information, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring

[37] *Id*.

[38] GAO, *Report to Congressional Requesters*, at 29 (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited June 11, 2024).

them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

81. LivaNova's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their Private Information, for which there is a well-established national and international market;

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach; and

i. nominal damages.

82. While Plaintiff's and Class Members' Private Information has been stolen, LivaNova continues to hold Plaintiff's and Class Members' Private Information. Particularly because LivaNova have demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

H. Plaintiff's Experience.

83. Plaintiff Crystal Schultz was a customer of LivaNova and gave them PHI.

84. Plaintiff provided Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information.

85. Plaintiff received a Notice Letter from LivaNova concerning the Data Breach dated May 31, 2024, which informed her that her Private Information had been compromised in the Data Breach.

86. Since the Data Breach, Plaintiff has noticed a marked spike in spam texts asking

her to respond. She has experienced anxiety and increased concerns for the loss of her privacy, as well as anxiety over the impact of cybercriminals accessing and using her Private Information.

87. Since the Data Brach, Plaintiff noticed fraudulent charges on her debit card which resulted in her having to replace her card twice.

88. Plaintiff would not have entrusted her Private Information to her healthcare provider had she known LivaNova would not take reasonable steps to safeguard her information.

89. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

90. Plaintiff is very careful about sharing sensitive Private Information. She stores documents containing Private Information in safe and secure locations and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Plaintiff would not have entrusted her Private Information to her healthcare provider had she known of LivaNova's lax data security policies.

91. As a direct and proximate result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts.

92. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

CLASS ALLEGATIONS

93. Plaintiff brings this class action individually on behalf of herself and on behalf of all members of the following Class of similarly situated persons pursuant to Federal Rule of Civil

Procedure 23. Plaintiff seeks certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3) of the following Class:

> All persons residing in the United States whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

94. Excluded from the Class are LivaNova and its affiliates, parents, subsidiaries, officers, agents, and directors, any entities in which LivaNova has a controlling interest, as well as the judge(s) presiding over this matter and the clerks, judicial staff, and immediate family members of said judge(s).

95. Plaintiff reserves the right to modify or amend the foregoing Class definitions before the Court determines whether certification is appropriate.

96. Numerosity: The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. As noted above, it has been reported that approximately 11 million individuals' information was exposed in the Data Breach.

97. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. These common questions of law or fact include, *inter alia*:

a. Whether LivaNova engaged in the conduct alleged herein;

b. Whether LivaNova had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' Private Information from unauthorized access and disclosure;

c. Whether LivaNova's computer systems and data security practices used to protect Plaintiff's and Class Members' Private Information violated the FTC Act and/or state laws, and/or LivaNova's other duties discussed herein;

d. Whether LivaNova failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

e. Whether LivaNova unlawfully shared, lost, or disclosed Plaintiff's and Class Members' Private Information;

f. Whether LivaNova's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether LivaNova's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Plaintiff and Class Members suffered injury as a proximate result of LivaNova's negligent actions or failures to act;

i. Whether LivaNova failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' Private Information;

j. Whether LivaNova breached duties to protect Plaintiff's and Class Members' Private Information;

k. Whether LivaNova's actions and inactions alleged herein were negligent;

l. Whether LivaNova were unjustly enriched by their conduct as alleged herein;

m. Whether an implied contract existed between Class Members and LivaNova with respect to protecting Private Information and privacy, and whether that contract was breached;

n. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages or other relief, and the measure of such damages and relief;

o. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

p. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

98. LivaNova engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of herself and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

99. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her Private Information compromised in the Data Breach. Plaintiff and Class Members were injured by the same wrongful acts, practices, and omissions committed by LivaNova, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

100. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class Members. Plaintiff is an adequate representative of the Class and has no interests adverse to, or conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

101. Superiority: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered

in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against LivaNova, so it would be impracticable for Class Members to individually seek redress from LivaNova's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

102. Injunctive and Declaratory Relief: LivaNova has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

103. Likewise, particular issues are appropriate for certification under Rule 24(c)(4) because such claims present only particular, common issues, the resolution of which would advance the disposition of this mater and the parties' interests therein. Such issues include, but are not limited to: (a) whether LivaNova owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, and safeguarding their Private Information; (b) whether LivaNova failed to adequately monitor and audit their data security systems; and (c) whether LivaNova failed to take reasonable steps to safeguard the Private Information of Plaintiff and Class Members.

104. All members of the proposed Class are readily ascertainable. LivaNova has access to the names in combination with addresses and/or e-mail addresses of Class Members affected by the Data Breach. Indeed, impacted Class Members already have been preliminarily identified and sent a breach notice letter.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

105. Plaintiff restates and realleges paragraphs 1 through 104 above as if fully set forth herein.

106. LivaNova's clients require their customers to submit non-public Private Information as a condition of receiving its products.

107. LivaNova gathered and stored the Private Information of Plaintiff and Class Members as part of its business, which affects commerce.

108. Plaintiff and Class Members, through their healthcare providers, entrusted LivaNova with their Private Information with the understanding that the information would be safeguarded.

109. LivaNova had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if their Private Information were wrongfully disclosed.

110. By assuming the responsibility to collect and store this data, LivaNova had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

111. LivaNova owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

112. LivaNova's duty to use reasonable security measures arose as a result of the special relationship that existed between LivaNova, on the one hand, and Plaintiff and Class Members, on the other hand. That special relationship arose because LivaNova was entrusted with their confidential Private Information, a necessary part of medical products, and LivaNova (and possibly other employers) shared the information with LivaNova.

113. LivaNova also had a duty to exercise appropriate clearinghouse practices to remove clients' former patients' Private Information they were no longer required to retain pursuant to regulations.

114. Moreover, LivaNova had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach, but failed to do so.

115. LivaNova had and continues to have duties to adequately disclose that Plaintiff's and Class Members' Private Information within LivaNova's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

116. LivaNova breached its duties and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by LivaNova include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove clients' former patients' Private Information they were no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

117. LivaNova breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

118. LivaNova knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and the Class.

119. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

120. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of LivaNova's inadequate security practices.

121. It was foreseeable that LivaNova's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of corporate cyberattacks and data breaches.

122. LivaNova had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

123. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. LivaNova knew or should have known of the inherent risks in collecting and storing Private Information, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on its systems.

124. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, LivaNova's possession.

125. LivaNova was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

126. LivaNova's duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

127. LivaNova has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

128. But for LivaNova's wrongful and negligent breaches of duties owed to Plaintiff and the Class, Plaintiff's and Class Members' Private Information would not have been compromised.

129. There is a close causal connection between LivaNova's failure to implement security measures to protect Plaintiff's and Class Members' Private Information, and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. Private Information was lost and accessed as the proximate result of LivaNova's failure to exercise reasonable care by adopting, implementing, and maintaining appropriate security measures.

130. As a direct and proximate result of LivaNova's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in LivaNova's possession and is subject to further unauthorized disclosures so long as LivaNova fails to undertake appropriate and adequate measures to protect the Private Information; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by LivaNova's data breach; (x) the value of the unauthorized access to their PII/PHI permitted by Defendant; and (xi) any nominal damages that may be awarded.

131. As a direct and proximate result of LivaNova's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses including nominal damages.

132. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

133. LivaNova's negligent conduct is ongoing, in that it still possesses Plaintiff's and Class Members' Private Information in an unsafe and insecure manner.

134. Plaintiff and Class Members are entitled to injunctive relief requiring LivaNova to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

135. Plaintiff restates and realleges paragraphs 1 through 104 above as if fully set forth herein.

136. LivaNova had duties arising under HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and the FTC Act to protect Plaintiff's and Class Members' Private Information.

137. LivaNova breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by LivaNova include, but are not limited to, the following: (i) failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information; (ii) failing to adequately monitor the security of their networks and systems; (iii) allowing unauthorized access to Class Members' Private Information; (iv) failing to detect in a timely manner that Class Members' Private Information had been compromised; (v) failing to remove clients' former patients' Private Information they were no longer required to retain pursuant to regulations; and

(vi) failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

138. LivaNova's violation of HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

139. Plaintiff and Class Members are consumers within the class of persons that HIPAA, HITECH, and Section 5 of the FTC Act were intended to protect.

140. The harm that has occurred is the type of harm HIPAA, HITECH, and the FTC Act were intended to guard against.

141. The FTC has pursued enforcement actions against businesses and healthcare entities that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

142. LivaNova breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

143. In addition, under state data security and consumer protection statutes such as those outlined herein, LivaNova had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Private Information.

144. Plaintiff and Class Members were foreseeable victims of LivaNova's violations of HIPAA, HITECH, and the FTC Act, and state data security and consumer protection statutes. LivaNova knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and the Class.

145. As a direct and proximate result of LivaNova's negligence per se, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in LivaNova's possession and is subject to further unauthorized disclosures so long as LivaNova fails to undertake appropriate and adequate measures to protect the Private Information.

146. As a direct and proximate result of LivaNova's negligence per se Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

147. Finally, as a direct and proximate result of LivaNova's negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in LivaNova's possession and is subject to further unauthorized disclosures so long as LivaNova fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

COUNT III
BREACH OF THIRD-PART BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Class)

148. Plaintiff restates and realleges paragraphs 1 through 104 above as if fully set forth herein.

149. On information and belief, LivaNova entered into contracts to sell its products to its customers (medical providers), and those contracts included an obligation to implement data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be provided to it.

150. On information and belief, these contracts are virtually identical and were made expressly for the benefit of Plaintiff and the Class, as it was their Private Information that LivaNova agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties.

151. LivaNova knew that if it were to breach these contracts with its clients, the clients' members, including Plaintiff and the Class Members, would be harmed.

152. LivaNova breached its contracts with its customers—whose patients, including Plaintiff and the Class Members—were affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach, and when it failed to timely notify Plaintiff and Class Members regarding the breach.

153. As foreseen, Plaintiff and the Class Members were harmed by LivaNova's failure to use reasonable data security measures to store the Private Information Plaintiff and Class Members provided to their respective health plans or other entities who in turn provided that information to LivaNova and the failure to timely notify Plaintiff and Class Members, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

154. Accordingly, Plaintiff and the Class Members are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages, along with costs and attorneys' fees incurred in this action.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

155. Plaintiff restates and realleges paragraphs 1 through 104 above as if fully set forth herein.

156. This count is pleaded in the alternative to the breach of third-party beneficiary contract claim above against LivaNova (Count III).

157. Plaintiff and Class Members conferred a monetary benefit on LivaNova in connection with obtaining medical products, specifically providing LivaNova with their Private Information.

158. LivaNova knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. LivaNova profited from Plaintiff's retained data and use Plaintiff's and Class Members' Private Information for business purposes.

159. LivaNova failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

160. LivaNova acquired the Private Information through inequitable record retention as it failed to disclose the inadequate vendor vetting and data security practices previously alleged.

161. Under the circumstances, it would be unjust for LivaNova to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

162. As a direct an proximate result of LivaNova's conduct, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in LivaNova's possession and is subject to further unauthorized disclosures or further entrustment to inadequate third party vendors so long as LivaNova fails to undertake appropriate and adequate measures to protect the Private Information; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by LivaNova's data breach; (x) the value of the unauthorized access to their PII/PHI permitted by Defendant; and (xi) any nominal damages that may be awarded.

163. Plaintiff and Class Members are entitled to restitution and/or damages from LivaNova and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by LivaNova from its wrongful conduct, as well as return of their sensitive Private Information and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

164. Plaintiff and Class Members may not have an adequate remedy at law against LivaNova, and accordingly, they plead this claim for unjust enrichment in addition to, or in the

alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the class, respectfully requests that the Court enter judgment in Plaintiff's favor and against LivaNova as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representatives, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, nominal damages and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the class, seek appropriate injunctive relief designed to prevent LivaNova from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: June 17, 2024

Respectfully submitted,

/s/ Joe Kendall
Joe Kendall
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC

3811Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

Jeff Ostrow (*pro hac vice* forthcoming)
Kenneth Grunfeld (*pro hac vice* forthcoming)
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
E: ostrow@kolawyers.com
grunfeld@kolawyers.com

Counsel for Plaintiff and the Proposed Class