UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

JAMIE CALVERT, individually and on behalf of all others similarly situated, Plaintiff, v. ZOLL MEDICAL CORPORATION, Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jamie Calvert, individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through his attorneys, brings this Class Action Complaint against Defendant ZOLL Medical Corporation ("ZOLL"), and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against ZOLL for its failure to secure and safeguard his and approximately 1,004,443 other individuals' personally identifying information ("PII") and personal health information ("PHI"), including name, address, date of birth, Social Security number, and information that a person was a user or was considered for use of a ZOLL product.

2. ZOLL is a company that develops and sells medical products, including defibrillators, ventilators, aspirators, and cardiac monitors. The company is headquartered in Chelmsford, Massachusetts.

3. Between January 28, 2023 and February 2, 2023, an unauthorized individual, or unauthorized individuals, gained access to ZOLL's network systems and accessed and acquired

files from the system that contained the PII/PHI of Plaintiff and Class members (the "Data Breach").

4. ZOLL owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. ZOLL breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its customers' PII/PHI from unauthorized access and disclosure.

5. As a result of ZOLL's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all persons whose PII/PHI was exposed as a result of the Data Breach.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, breach of fiduciary duty, breach of implied contract, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Jamie Calvert

7. Plaintiff Jamie Calvert is a Tennessee resident.

8. Plaintiff Calvert purchased a product from ZOLL in late 2017. As a condition of purchasing the product, ZOLL required Plaintiff Calvert to provide ZOLL with his PII/PHI.

9. Based on representations made by ZOLL, Plaintiff Calvert believed that ZOLL had implemented and maintained reasonable security and practices to protect his PII/PHI. With this

belief in mind, Plaintiff Calvert provided his PII/PHI to ZOLL in connection with and in exchange for purchasing a product from ZOLL.

10. In connection with services provided to Plaintiff, ZOLL stores and maintains Plaintiff's PII/PHI on its systems, including the system involved in the Data Breach.

11. Had Plaintiff Calvert known that ZOLL does not adequately protect the PII/PHI in its possession, he would not have agreed to provide ZOLL with his PII/PHI or would not have used ZOLL's services.

12. Plaintiff Calvert received a letter from ZOLL notifying him that his PII/PHI was exposed in the Data Breach.

13. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

Defendant ZOLL Medical Corporation

14. Defendant ZOLL Medical Corporation is a Massachusetts corporation with its principal place of business in Chelmsford, Massachusetts. ZOLL's headquarters are located at 269 Mill Road, Chelmsford, MA 01824. ZOLL may be served through its registered agent: Corporation Service Company, 84 State Street, Boston, Massachusetts 02109.

JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from ZOLL, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

16. This Court has personal jurisdiction over ZOLL Medical Corporation because ZOLL Medical Corporation has its principal place of business in Massachusetts.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because ZOLL's principal place of business is in Massachusetts and a significant amount of the events leading to Plaintiff's causes of action occurred in this District.

FACTUAL ALLEGATIONS

Overview of ZOLL

18. ZOLL "develops and markets medical devices and software solutions."[1] ZOLL provides "products for defibrillation and cardiac monitoring, circulation enhancement and CPR feedback, supersaturated oxygen therapy, data management, ventilation, therapeutic temperature management, and sleep apnea diagnosis and treatment."[2] In the regular course of its business, ZOLL collects and maintains the PII/PHI of its customers.

19. ZOLL's website states that the company "respects the privacy of its customers, employees, business partners, and individuals whose personal information with which we are entrusted" and that it "collects and uses any collected personal health information in accordance with the laws and regulations of the countries in which the information is collected."[3] ZOLL's website also has a privacy policy (the "Privacy Policy"), which states, "We have implemented measures designed to secure your personal information from accidental loss and from unauthorized access, use, alteration, and disclosure."[4]

---

[1] *Company Overview*, ZOLL, https://www.ZOLL.com/about-ZOLL/company-overview (last accessed Mar. 21, 2023).
[2] *Id*.
[3] *Compliance*, ZOLL, https://www.ZOLL.com/about-ZOLL/compliance (last accessed Mar. 21, 2023).
[4] *Privacy Policy*, ZOLL, https://www.ZOLL.com/privacy-policy (last accessed Mar. 21, 2023)

20. Plaintiff and Class members are, or were, customers of ZOLL and entrusted ZOLL with their PII/PHI.

The Data Breach

21. Between January 28, 2023 and February 2, 2023, an unauthorized individual, or unauthorized individuals, gained access to ZOLL's network systems and accessed and acquired certain files on ZOLL's computer systems.

22. The Data Breach impacted the PII/PHI of certain of ZOLL's current and former customers. In particular, the Data Breach affected persons who were considered for use of a ZOLL produce called the LifeVest device, which is a "wearable cardioverter defibrillator."[5]

23. ZOLL began notifying affected persons on March 10, 2023. The notice letter states that the information that the cybercriminal had access to includes the following PII/PHI: "name, address, date of birth, and Social Security number."[6] The letter goes on to state, "It may also be inferred that you used or were considered for use of a ZOLL product."[7]

ZOLL Knew that Criminals Target PII/PHI

24. At all relevant times, ZOLL knew, or should have known, that the PII/PHI that it collected was a target for malicious actors. Despite such knowledge, ZOLL failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that ZOLL should have anticipated and guarded against.

---

[5] Jessica Davis, *ZOLL Medical Notifies 1M Patients of Data Breach Tied to LifeVest Device*, SC MEDIA (Mar. 14, 2023), https://www.scmagazine.com/news/privacy/ZOLL-medical-notifies-1m-patients-data-breach-lifevest-device.
[6] *See* https://www.mass.gov/doc/assigned-data-breach-number-29194-ZOLL-medical-corporation/download (last accessed Mar. 21, 2023).
[7] *Id*.

25. It is well known among companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers ("SSNs") and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[8]

26. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient records exposed.[9] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[10]

27. PII/PHI is a valuable property right.[11] The value of PII/PHI as a commodity is measurable.[12] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[13] American companies are estimated to have spent over $19 billion on acquiring

---

[8] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[9] *See* PROTENUS, *2023 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last accessed Mar. 21, 2023).
[10] *See id*.
[11] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.
[12] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.
[13] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

personal data of consumers in 2018.[14] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

28. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

29. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[15] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[16]

30. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[17] According to a report released by the Federal Bureau of Investigation's

[14] *See* IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[15] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data*") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[16] *Id.*

[17] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[18]

31. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[19] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[20]

32. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[21]

33. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[18] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[19] *What Happens to Stolen Healthcare Data*, *supra* n.15.

[20] *Id.*

[21] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

34. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[22]

35. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[23] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[24]

36. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the

---

[22] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Mar. 21, 2023).

[23] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). 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," 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." 12 C.F.R. § 1022.3(g).

[24] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Mar. 21, 2022).

victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.[25]

37. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[26]

38. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

39. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[27]

40. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records

[25] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Mar. 21, 2023).
[26] *See* Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Mar. 21, 2022).
[27] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

that can plague victims' medical and financial lives for years."[28] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[29] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [30] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[31]

41. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services neither sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

---

[28] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[29] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* n.18.
[30] *See What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Mar. 21, 2023).
[31] *Id*.

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[32]

42. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[33]

43. It is within this context that Plaintiff and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by and in the possession of people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

44. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in ZOLL's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the

[32] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* n.28.
[33] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

45. This action is brought and may be properly maintained as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

46. Plaintiff brings this action on behalf of himself and all members of the following Nationwide Class of similarly situated persons:

> All persons whose personally identifiable information or personal health information was compromised in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

47. Excluded from the Class are ZOLL Medical Corporation and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

48. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

49. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. ZOLL reported to the Maine Attorney General that approximately 1,004,443 persons' information was exposed in the Data Breach.[34]

50. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

[34] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/ab192c35-667d-4bc9-ad18-fa710bd10b15.shtml (last accessed Mar. 21, 2023).

a. Whether ZOLL had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether ZOLL had duties not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. Whether ZOLL failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d. Whether an implied contract existed between Class members and ZOLL, providing that ZOLL would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

e. Whether ZOLL engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiff and Class members;

f. Whether ZOLL breached its duties to protect Plaintiff's and Class members' PII/PHI; and

g. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

51. ZOLL engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself 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.

52. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII/PHI compromised in the Data Breach. Plaintiff and Class

members were injured by the same wrongful acts, practices, and omissions committed by ZOLL, 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.

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

54. 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 Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against ZOLL, so it would be impracticable for Class members to individually seek redress from ZOLL'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.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

55. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

56. ZOLL owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding, securing, and protecting the PII/PHI in their possession, custody, or control.

57. ZOLL's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA 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 (collectively, "HIPAA Privacy and Security Rules"). Plaintiff and Class members are the persons that the HIPPA Privacy and Security Rules were intended to protect and the harm that Plaintiff and Class members suffered is the type of harm the rules were intended to guard against.

58. ZOLL's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as ZOLL, of failing to employ reasonable measures to protect and secure PII/PHI. Plaintiff and Class members are the persons that the Section 5 of the FTCA was intended to protect and the harm that Plaintiff and Class members suffered is the type of harm Section 5 of the FTCA intended to guard against.

59. ZOLL knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems.

ZOLL knew or should have known of the many data breaches that have targeted companies that stored PII/PHI in recent years.

60. Given the nature of ZOLL's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, ZOLL should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

61. ZOLL makes explicit statements on its website that it will follow privacy laws and regulations and use reasonable methods to protect the PII/PHI in its control.

62. ZOLL breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to them—including Plaintiff's and Class members' PII/PHI.

63. Plaintiff and Class members had no ability to protect their PII/PHI that was, or remains, in ZOLL's possession.

64. It was or should have been reasonably foreseeable to ZOLL that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

65. But for ZOLL's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised. The PII/PHI of Plaintiff and the Class was lost and accessed as the proximate result of ZOLL's failure to exercise

reasonable care in safeguarding, securing, and protecting such PII/PHI by, *inter alia*, adopting, implementing, and maintaining appropriate security measures.

66. As a result of ZOLL's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in ZOLL's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
BREACH OF FIDUCIARY DUTY

67. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

68. As a condition of obtaining services from ZOLL, Plaintiff and Class members gave ZOLL their PII/PHI in confidence, believing that ZOLL would protect that information. Plaintiff and Class members would not have provided ZOLL with this information had they known it would not be adequately protected. ZOLL's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between ZOLL and Plaintiff and Class members. In light of this relationship, ZOLL must act primarily for the benefit of its

customers, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

69. ZOLL has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected.

70. As a direct and proximate result of ZOLL's breach of their fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in ZOLL's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF IMPLIED CONTRACT

71. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

72. In connection with receiving health care services, Plaintiff and all other Class members entered into implied contracts with ZOLL.

73. Pursuant to these implied contracts, Plaintiff and Class members paid money to ZOLL and provided ZOLL with their PII/PHI. In exchange, ZOLL agreed to, among other things, and Plaintiff understood that ZOLL would: (1) provide products or services to Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

74. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and ZOLL, on the other hand. Indeed, as set forth *supra*, ZOLL recognized the importance of data security and the privacy of its customers' PII/PHI on its website and in its Privacy Policy. Had Plaintiff and Class members known that ZOLL would not adequately protect its customers' and former customers' PII/PHI, they would not have paid for products or services from ZOLL.

75. Plaintiff and Class members performed their obligations under the implied contract when they provided ZOLL with their PII/PHI and paid for products and services from ZOLL, expecting that their PII/PHI would be protected.

76. ZOLL breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

77. ZOLL's breach of its obligations of the implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the resulting injuries to Plaintiff and Class members.

78. Plaintiff and all other Class members were damaged by ZOLL's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they now face a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

COUNT IV
UNJUST ENRICHMENT

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. This claim is pleaded in the alternative to the breach of implied contract claim.

81. In obtaining services from ZOLL, Plaintiff and Class members provided and entrusted their PII and PHI to ZOLL.

82. Plaintiff and Class members conferred a monetary benefit upon ZOLL in the form of monies paid for products or services, with an implicit understanding that ZOLL would use some of its revenue to protect the PII/PHI it collects.

83. ZOLL accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. ZOLL also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate billing and payment services.

84. As a result of ZOLL's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

85. ZOLL should not be permitted to retain the money belonging to Plaintiff and Class members because ZOLL failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

86. ZOLL should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against ZOLL as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, 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, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent ZOLL from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide

or extend credit monitoring services and similar services to protect against all types of identity theft and medical 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 DEMANDED

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

Dated: March 22, 2023

Respectfully submitted,

/s/ David Pastor

David Pastor (BBO 391000)
Pastor Law Office, PC
63 Atlantic Avenue, 3rd Floor
Boston, MA 02110
Tel: 617.742.9700
Fax: 617.742.9701
dpastor@pastorlawoffice.com

Ben Barnow*
Anthony L. Parkhill*
Riley W. Prince*
Barnow and Associates, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com
rprince@barnowlaw.com

Counsel for Plaintiff Jamie Calvert

* *pro hac vice forthcoming*