IN THE UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
EASTERN DIVISION

ROBERT SMITH, JOHN PRIDDY, RANDY MCGILBERRY, TIMOTHY JEMISON, NATHANIEL GERTH, GARY BECKER, AMINE M. BENDRISS, BARBARA BROWN, DAVID PACHOLCZAK, PATRICIA MCMAHON, and EVAN WEESE, on behalf of themselves and others similarly situated, Plaintiffs, v. **ZOLL MEDICAL CORPORATION,** Defendant.	Case No. 1:23-cv-10575-IT **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs John Priddy, Randy McGilberry, Timothy Jemison, Nathaniel Gerth, Gary Becker, Amine M. Bendriss, Barbara Brown, David Pacholczak, Patricia McMahon, and Evan Weese,[1] individually and on behalf of the Classes defined below of similarly situated persons ("Plaintiffs and Class Members"), allege the following against Defendant Zoll Medical Corporation, ("Zoll" or "Defendant"). The following allegations are based on Plaintiffs' knowledge, investigations by Plaintiffs' counsel, facts of public record, and information and belief:

NATURE OF THE ACTION

1. Plaintiffs seek to hold Defendant responsible for the injuries Zoll inflicted on Plaintiffs and over one million others due to Defendant's egregiously inadequate data security,

[1] Robert Smith, who had filed the first proceeding in this consolidated action, is dismissing his claims against Zoll and is therefore not included in this Consolidated Complaint.

which resulted in the private information of Zoll's current and former patients and employees, including Plaintiffs and those similarly situated, to be exposed to unauthorized third parties (the "Data Breach").

2. Zoll produces and sells a variety of advanced emergency care devices that provide defibrillation and cardiac monitoring, circulation enhancement and CPR feedback, supersaturated oxygen therapy, ventilation, and more. In the course and scope of providing, servicing, and monitoring those devices, Zoll collects sensitive personal and health information from its patients. In the course and scope of its operations, Zoll collects sensitive personal information from its employees.

3. The data that Zoll exposed to the public is unique and highly sensitive. For one, the exposed data included personal identifying information ("PII") and protected health information ("PHI") like Social Security numbers, full names, dates of birth, and addresses, which Plaintiffs and Class Members provided to Zoll with the understanding Zoll would keep that information private in accordance with both state and federal laws.

4. The exposed data also allowed individuals to infer that Plaintiffs and Class Members were using or being considered for certain Zoll products, thereby disclosing their medical conditions. The fact that an individual received a medical service is itself PHI, and in the present situation, some of the data is linked to medical equipment associated with specific mediation conditions.

5. Indeed, the information compromised in the Data Breach represents a gold mine for data thieves.

6. According to Zoll, on January 28, 2023, Zoll detected unusual activity on its internal computer network. On or about February 2, 2024, Zoll was able to confirm that security and privacy of Plaintiffs' and Class Members' PII and PHI was impacted.

7. 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 entities like Zoll 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.

8. Instead of abiding by these industry and regulatory standards, however, Zoll disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. Zoll's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

9. Exacerbating the injuries to Plaintiffs and Class Members, Zoll failed to provide timely notice to Plaintiffs and Class Members, depriving them of the chance to take speedy measures to protect themselves and mitigate harm. When Zoll finally did notify Plaintiffs and Class Members of the disclosure nearly a month after discovering the Data Breach, Zoll offered scant details about the Data Breach, no assurances that all personal data or copies of data have been recovered or destroyed, or that Zoll has adequately enhanced its security practices or dedicated sufficient resources and staff to avoid a breach of its network in the future. In fact, as

detailed herein, Zoll has experienced additional security breaches affecting PII and PHI since the Data Breach, suggesting Zoll *still* does not have adequate security practices in place.

10. Today, the PII and PHI of Plaintiffs and Class Members continue to be in jeopardy because of Defendant's actions and inactions described herein. Because their personal and sensitive data is now in the hands of cybercriminals, Plaintiffs and Class Members now suffer from a heightened and imminent risk of fraud and identity theft for years to come and now must constantly monitor their medical and financial accounts for unauthorized activity.

11. The PII and PHI (collectively "Private Information") exposed in the Data Breach, including social security numbers and health information, can enable criminals to commit a litany of crimes. Criminals can open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' health information to craft phishing and other hacking attacks based on Class Members' individual health needs, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

12. As a result of the Data Breach, Plaintiffs and Class Members face a substantial risk of imminent and certainly impending harm. Plaintiffs and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

13. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach.

14. As a direct and proximate result of the Data Breach, Plaintiffs 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 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) anxiety, annoyance, and nuisance; (k) continued risk to their Private Information, which remains in Zoll's possession and is subject to further breaches so long as Zoll fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information; and (l) disgorgement damages associated with Zoll's maintenance and use of Plaintiffs' data for its benefit and profit.

15. Through this action, Plaintiffs seek to remedy these injuries on behalf of themselves and all similarly situated individuals whose Private Information was exposed and compromised in the Data Breach.

16. Plaintiffs bring this action against Zoll and assert claims for negligence, negligence *per se*, unjust enrichment, breach of fiduciary duty, breach of contract, violations of various state statutes, and injunctive relief.

PARTIES

17. Plaintiff John Priddy is a natural person, resident, and citizen of Illinois.

18. Plaintiff Randy McGilberry is a natural person, resident, and citizen of Florida.

19. Plaintiff Timothy Jemison is a natural person, resident, and citizen of Texas.

20. Plaintiff Nathaniel Gerth is a natural person, resident, and citizen of Pennsylvania.

21. Plaintiff Gary Becker is a natural person, resident, and citizen of Kansas.

22. Plaintiff Amine M. Bendriss is a natural person, resident, and citizen of Pennsylvania.

23. Plaintiff Barbara Brown is a natural person, resident, and citizen of Florida.

24. Plaintiff David Pacholczak is a natural person, resident, and citizen of New York.

25. Plaintiff Patricia McMahon is a natural person, resident, and citizen of Illinois.

26. Plaintiff Evan Weese is a natural person, resident, and citizen of Texas.

27. Defendant Zoll Medical Corporation is a Massachusetts entity with a principal place of business and headquarters at 269 Mill Road, Chelmsford, Massachusetts.

JURISDICTION AND VENUE

28. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiffs (and many members of the Nationwide Class) are citizens of states different than Defendant.

29. This Court has general personal jurisdiction over Defendant because Defendant's principal place of business and headquarters are in Chelmsford, Massachusetts. Defendant also regularly conduct substantial business in Massachusetts.

30. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conduct substantial business in this District.

FACTUAL ALLEGATIONS

Zoll Collected and Stored the Private Information of Plaintiffs and Class Members

31. Zoll is part of the family of companies owned and operated by Japanese chemical company, Asahi Kasei. Zoll makes several advanced emergency care devices that provide defibrillation and cardiac monitoring, circulation enhancement and CPR feedback, supersaturated oxygen therapy, ventilation, associated software solutions, and more. Zoll "provide[s] innovative technologies that make a meaningful difference in people's lives. [Its] medical devices, software, and related services are used worldwide to diagnose and treat patients suffering from serious cardiopulmonary and respiratory condition."[2]

32. Zoll advertises that, "[w]ith 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, Zoll provides a comprehensive set of technologies that help clinicians, EMS and fire professionals, as well as lay rescuers, improve patient outcomes in critical cardiopulmonary conditions."[3]

33. Plaintiffs and Class Members provided their Private Information to Zoll in conjunction with the type of work Zoll does within the healthcare industry.

34. Zoll collects Private Information from Plaintiffs and Class Members such as their full names, Social Security Numbers, address, date of birth, and some medical information in the ordinary course of business, including data transmitted through Zoll's medical devices for purposes of monitoring and diagnostic analysis. Upon information and belief, this Private Information is then stored on Defendant's computer network.

---

[2] *Company Overview*, Zoll Med. Corp., https://www.zoll.com/about-zoll/company-overview (last accessed Feb. 22, 2024).
[3] *See id*.

35. Because of the highly sensitive and personal nature of the information Zoll acquires and stores, Zoll knew or reasonably should have known that it must comply with healthcare industry standards related to data security and all federal and state laws protecting Private Information and provide adequate notice if Private Information is disclosed without proper authorization.

36. Because of the highly sensitive and personal nature of the information Zoll acquires and stores with respect to patients and other individuals, Zoll, upon information and belief, promises to, among other things: keep Private Information private; comply with health care industry standards related to data security and Private Information, including HIPAA; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to medical care and treatment; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

37. As HIPAA covered business entities (*see infra*), Zoll is required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

38. However, Zoll did not maintain adequate security to protect their systems from infiltration by cybercriminals and waited to publicly disclose the Data Breach.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Zoll assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private

Information from unauthorized disclosure.

40. Recognizing its legal and equitable duties, Zoll represents in its Privacy Policy that it "[has] implemented measures designed to secure [Plaintiffs' and Class Members'] personal information from accidental loss and unauthorized access, use, alteration, and disclosure."[4] Zoll misrepresented to Plaintiffs and Class Members via its Privacy Policy that it has implemented measures to protect from theft and misuse Plaintiffs' and Class Members' Private Information. Upon information and belief, including from information gathered from the Data Breach at issue and subsequent cybersecurity issues within Zoll's computer network, that representation is not true.

41. Plaintiffs and Class Members provided their Private Information to Zoll as a condition of receiving products and services from Zoll, but in doing so, expected Zoll to keep their Private Information confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

The Data Breach

42. The Notice of Data Breach Letter provided by Zoll to Plaintiffs and Class Members nearly a month after the Data Breach was first discovered states:

> On January 28, 2023, we detected unusual activity on our internal network, and we promptly took steps to mitigate the incident. We consulted with third-party cybersecurity experts to assist with our response to the incident, and we notified law enforcement. We determined that your information may have been affected on or about February 2, 2023. Our investigation into the incident is ongoing.[5]

43. The letter further states:

[4] *Privacy Policy*, Zoll Med. Corp., ttps://www.zoll.com/privacy-policy#d (last accessed Feb. 21, 2024).
[5] Ex. 1, Notice of Data Breach.

> Information that may have been disclosed includes your name, address, date of birth, and Social Security number. It may also be inferred that you used or were considered for use of a ZOLL product.[6]

44. Upon information and belief, Plaintiffs' and Class Members' affected Private Information at the time of the Data Breach was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

45. Upon information and belief, Zoll was a target by due to Zoll's status as healthcare related entity that collects, creates, and maintains Private Information.

46. The Notice Letter does not detail to Plaintiffs nor Class Members how their Private Information was disclosed and, thus, leaves Plaintiffs and Class Members wondering how they can protect themselves.

47. Time is of the essence when highly sensitive Private Information is subject to unauthorized access and/or acquisition. Hackers can access and then offer for sale the unencrypted, unredacted Private Information to other criminals and victims must be vigilant to protect themselves from further fraud and injury.

48. Plaintiffs and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their Private Information, especially their Social Security numbers and sensitive medical information, onto the Dark Web. Plaintiffs and Class Members face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Social Security numbers and/or specific, sensitive medical information.

---

[6] *See id.*

49. Zoll largely put the burden on Plaintiffs and Class Members to take measures to protect themselves from identity theft and fraud without giving any details as to what the unauthorized access was or who may not have possession of their Private Information.

50. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[7]

51. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[8] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[9] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, Plaintiffs and Class Members now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

52. Plaintiffs and Class Members are deprived of the choice as to how to spend their valuable free hours and therefore seek renumeration for the loss of valuable time as another element of damages.

---

[7] *Characteristics of minimum wage workers,* U.S. BUREAU OF LABOR STATISTICS (2020), https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed Jan. 30, 2023).

[8] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC (Nov. 6, 2019), https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html.

[9] *Id.*

53. Defendant offered identity monitoring services for a period of 24 months. Such measures, however, are insufficient to protect Plaintiffs and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiffs and Class Members seek a sum of money sufficient to provide to Plaintiffs and Class Members identity theft protection services for their respective lifetimes.

54. Plaintiffs and the Class Members remain, even over a year later, in the dark regarding exactly what data was stolen, the particular method of disclosure, the results of any investigations, and what steps are being taken, if any, to secure their Private Information going forward. Plaintiffs and Class Members are left to speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

55. Zoll could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiffs' and Class Members' Private Information.

56. Defendant's negligence in safeguarding Plaintiffs' and Class Members' PII and PHI was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

57. As HIPAA covered business entities (*see infra*) that collect, create, and maintain significant volumes of Private Information, the targeted attack was a foreseeable risk which Zoll was aware of and which Zoll knew they had a duty to guard against. It is well-known that healthcare businesses such as Defendants', which collect and store the confidential and sensitive PII/PHI of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity

safeguards.

58. The healthcare industry has experienced a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint, and cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[10] According to the HIPAA Journal, the largest healthcare data breaches have been reported beginning in April 2021.[11]

59. In the context of data breaches, healthcare is "by far the most affected industry sector."[12] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[13] And according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[14]

60. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiffs' and Class Members' Private Information from being compromised.

61. Zoll had obligations created by HIPAA, contract, industry standards, common law, and their own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

---

[10] *2020 Healthcare Data Exposure Report*, HIPAA JOURNAL (Jan. 19, 2021) https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/.
[11] *April 2021 Healthcare Data Exposure Report*, HIPAA JOURNAL (May 18, 2021) https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/.
[12] Tenable Security Response Team, *Healthcare Sec.*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.
[13] *See id.*
[14] *See* Maria Henriquez, *Iowa City Hosp. Suffers Phishing Attack*, SEC. MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

62. Plaintiffs and Class Members provided their Private Information to Zol, either directly or indirectly, with the reasonable expectation and mutual understanding that Zoll would comply with their obligations to keep such information confidential and secure from unauthorized access.

63. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Zoll assumed legal and equitable duties and knew, or should have known, that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

64. Due to Zoll's inadequate security measures and delayed notice to victims, Plaintiffs and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

65. Zoll failed to properly train its employees as to cybersecurity best practices and to maintain proper staffing and processes for responding to and preventing network intrusions.

66. Zoll failed to implement sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

67. Zoll failed to encrypt Plaintiffs' and Class Members' Private Information and monitor user behavior and activity to identify possible threats.

68. Zoll failed to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

69. Zoll failed to timely and accurately disclose that Plaintiffs' and Class Members' PII and PHI had been improperly acquired or accessed.

70. Zoll knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII and PHI. These

standard industry, regulatory, and governmental standards for information security, as detailed *infra*, evidence a minimum duty and standard of care that Zoll should have followed to protect its repository of Private Information.

Zoll Failed to Comply with FTC Guidelines

71. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[15] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Zoll, should employ to protect against the unlawful exposure of Private Information.

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[16] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

73. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

74. The FTC recommends that companies: not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords

[15] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF.
[16] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre.

to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[17]

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp,* 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

77. Zoll's failure to employ reasonable and appropriate measures to protect against unauthorized access to Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45 and such failure serves as evidence of Zoll's negligence with regard to the Data Breah.

Zoll Failed to Follow Industry Standards

78. Despite its alleged commitments to securing sensitive data, Zoll does not follow industry standard practices in securing Private Information.

79. As shown above, experts studying cyber security routinely identify healthcare

[17] *See Start with Security*, *supra*.

related entities as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

80. Several best cybersecurity practices should be implemented by healthcare providers like Defendant, including but not limited to, educating all employees on the risks of cyber attacks; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

81. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

82. Upon information and belief, Zoll failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls ("CIS CSC"), which are all established standards in reasonable cybersecurity readiness.

83. Such frameworks are the existing and applicable industry standards in the healthcare industry. And Zoll failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

Zoll Violated HIPAA and HITECH

84. HIPAA circumscribes security provisions and data privacy responsibilities designed to safeguard medical information. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[18]

85. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[19]

86. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding

[18] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[19] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

87. Defendant recognizes that it is a business associate under HIPAA and agrees that it will comply with HIPAA.[20] The Data Breach, however, which resulted from a combination of insufficiencies, demonstrates that Defendant indeed failed to comply with safeguards mandated by HIPAA regulations.

88. Zoll 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.

89. Both HIPAA and HITECH obligate Zoll to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive 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.

Plaintiffs' Experiences and Injuries Caused by the Data Breach

90. Plaintiffs and Class Members are current and former patients/customers and/or employees of Zoll.

91. As a prerequisite of receiving medical devices or services from Zoll or engaging in employment with Zoll, Defendant required Plaintiffs and Class Members to provide their Private Information.

92. Zoll began notifying Plaintiffs and Class Members about the Data Breach on or around March 10, 2023—over one month after discovering the Data Breach.

93. When Zoll finally announced the Data Breach, it deliberately underplayed the severity and obfuscated the nature of the Data Breach. Defendant's Notice Letter fails to

[20] *See Business Associate Addendum*, Zoll Med. Corp., https://www.zolldata.com/business-associate-addendum (last accessed Feb. 21, 2024).

adequately explain how the breach occurred, what exact data elements of each affected individual were compromised, and the extent to which those data elements were compromised.

94. Because of the Data Breach, Defendant inflicted injuries upon Plaintiffs and Class Members. And yet, Defendant has done little to provide Plaintiffs and the Class Members with relief for the damages they suffered.

A. Plaintiff John Priddy

95. Plaintiff John Priddy is an adult individual and a natural person of Illinois, residing in Champaign County, where he intends to stay.

96. Zoll obtained Plaintiff's information through his use of a Zoll medical device, which was prescribed to him in or about 2015.

97. Plaintiff John Priddy received a notice letter from Defendant Zoll dated March 10, 2023 informing him of the Data Breach and the exposure of his Private Information.

98. The notice letter informed Plaintiff that his name, address, and date of birth, along with information regarding his use of the Zoll product, was potentially compromised in the Data Breach.

99. Plaintiff Priddy is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him, Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

100. Plaintiff John Priddy only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

101. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

102. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

103. Furthermore, Plaintiff has experienced a dramatic increase in the amount of spam he has been receiving, with some of the spam messages specifically relating to medical services or medical devices similar to Defendant's, as a result of the Data Breach.

104. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

105. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff spends approximately an hour every week since the Data Breach combing through his financial records, billing statements, and credit history to stay vigilant against potential fraud or identity theft.

106. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

107. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

B. Plaintiff Randy McGilberry

108. Plaintiff McGilberry is an adult individual and a natural person of Florida, where he intends to stay.

109. Plaintiff provided his information to Zoll through his use of a prescribed medical device manufactured and maintained by Defendant.

110. Plaintiff McGilberry received a notice letter from Defendant Zoll dated March 10, 2023, informing him of the Data Breach and the exposure of his Private Information.

111. The notice letter informed Plaintiff that his name, address, and date of birth, as well as his status as a user of a Zoll medical device, was potentially compromised in the Data Breach.

112. Plaintiff McGilberry is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online

accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

113. Plaintiff McGilberry only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

114. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

115. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

116. Upon information and belief, Plaintiff's Personal Information has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of numerous fraudulent charges to his debit card account, causing him to have to replace his card repeatedly. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

117. Furthermore, Plaintiff has experienced an increase in targeted spam as a result of the Data Breach, often directly using his private information obtained in the Data Breach.

118. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

119. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff has spent, and continues to spend, several hours speaking with his bank about fraudulent expenses, fraud alerts, canceling and reissuing his debit card, and reviewing his statements in an effort to remain vigilant.

120. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

121. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

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

C. Plaintiff Timothy Jemison

123. Plaintiff Timothy C. Jemison is an adult individual and a natural person of Texas, residing in Bowie County, where he intends to stay.

124. Plaintiff provided his information to Zoll when Plaintiff was prescribed, and used, a Zoll medical equipment product.

125. Plaintiff Jemison received a notice letter from Defendant Zoll dated March 10, 2023, informing him of the Data Breach and the exposure of his Private Information.

126. The notice letter informed Plaintiff that his name, address, date of birth, and health information such as the use of a Zoll product was potentially compromised in the Data Breach.

127. Plaintiff Jemison is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

128. Plaintiff Jemison only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

129. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

130. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was

placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

131. Upon information and belief, Plaintiff's Personal Information has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of fraudulent use of his debit cards from multiple bank accounts, unauthorized applications for credit cards, and medical bills issued under his name from unknown sources. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

132. Furthermore, Plaintiff has experienced frequent spam calls and text messages as a result of the Data Breach.

133. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

134. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff has incurred expenses related to late fees associated with various accounts due to the need to close and reopen new debit cards, and lost time relating to monitoring his credit and various accounts and reaching out to various financial institutions in response to discovered fraudulent activity.

135. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

136. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety including the need to check his accounts daily, if not multiple times a day, for fear of further fraudulent activity.

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

D. Plaintiff Nathaniel Gerth

138. Plaintiff Gerth is an adult individual and a natural person of Pennsylvania, residing in Allegheny County, where he intends to stay.

139. Plaintiff provided his information to Zoll as a condition of his employment with the company.

140. Plaintiff Gerth received a notice letter from Defendant Zoll dated March 10, 2023 informing him of the Data Breach and the exposure of his Private Information.

141. The notice letter informed Plaintiff that his name, address, and date of birth were potentially compromised in the Data Breach.

142. Plaintiff Gerth is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

143. Plaintiff Gerth only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

144. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

145. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

146. Upon information and belief, Plaintiff's Personal Information has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of fraudulent charges to his credit card accounts and debit card accounts, prompting him to have his cards reissued three times so far. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

147. Furthermore, Plaintiff has experienced a significant increase in spam and phishing attempts as a result of the Data Breach, with many attempts purporting to be from financial institutions and using some of the private information acquired in the Data Breach.

148. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

149. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff has spent approximately 60 hours so far reviewing his financial accounts weekly, checking unfamiliar charges to verify their legitimacy, communicating with his bank regarding fraudulent charges, investigating the Data Breach, and changing passwords to all of his online accounts.

150. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

151. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

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

E. Plaintiff Gary Becker

153. Plaintiff Becker is an adult individual and a natural person of Kansas, residing in Pottawatomie County, where he intends to stay.

154. Plaintiff provided his information to Zoll through his use of a prescribed medical device.

155. Plaintiff Becker received a notice letter from Defendant Zoll dated March 10, 2023 informing him of the Data Breach and the exposure of his Private Information.

156. The notice letter informed Plaintiff that his name, address, and date of birth was potentially compromised, along with his status as a user of a Zoll medical device, in the Data Breach.

157. Plaintiff Becker is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

158. Plaintiff Becker only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

159. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

160. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was

placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

161. Upon information and belief, Plaintiff's Personal Information has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of a notice from his bank of some fraudulent activity, as well as a separate fraudulent charge on his Wells Fargo card. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

162. Furthermore, Plaintiff has experienced a significant uptick in the amount of spam he has been receiving, with some spam directly trying to market unnecessary medical devices to him, as a result of the Data Breach. Plaintiff also received letters from Blue Cross Blue Shield related to a medical service that he never received and a transaction he never authorized.

163. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

164. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff has spent, to date, roughly 20 hours monitoring his credit card accounts and his bank accounts for any fraudulent activity. He has also signed up for a Norton and an Experian identity theft protection service as a result of the Breach, and regularly spends time reviewing those accounts for any notifications of fraud or attempted identity theft.

165. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring

his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

166. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

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

F. Plaintiff Amine M. Bendriss

168. Plaintiff Bendriss is an adult individual and a natural person of Pittsburgh, Pennsylvania, residing in Allegheny County, where she intends to stay.

169. Plaintiff provided her information to Zoll in connection with her use of a Zoll medical device.

170. Plaintiff Bendriss received a notice letter from Defendant Zoll dated March 10, 2023, informing her of the Data Breach and the exposure of her Private Information.

171. The notice letter informed Plaintiff that her name, address, and date of birth was potentially compromised in the Data Breach, along with her status as a user of a Zoll medical device.

172. Plaintiff Bendriss is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it

can be. When it is available to her Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

173. Plaintiff Bendriss only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

174. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

175. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

176. Plaintiff has also experienced an increase and shift in the amount and nature of spam she has been receiving. As a result of the Data Breach, Plaintiff now receives more spam than she did prior to the Data Breach, and the spam includes more phishing attempts targeted to obtain even more private information from her.

177. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

178. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff has spent several hours reaching out to her financial and credit institutions

to ensure that her accounts are secure and that the institutions know to be on the lookout for any suspicious transactions.

179. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

180. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

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

G. Plaintiff Barbara Brown

182. Plaintiff Barbara M. Brown is an adult individual and a natural person of Florida, residing in Duval County, where she intends to stay.

183. Plaintiff provided her information to Zoll in connection with a prescribed medical device.

184. Upon information and belief, Plaintiff Barbara M. Brown received a notice letter from Defendant Zoll on or about March 10, 2023, informing her of the Data Breach and the exposure of her Private Information.

185. Upon information and belief, the notice letter informed Plaintiff that her PII and PHI were potentially compromised in the Data Breach.

186. Plaintiff Barbara M. Brown is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

187. Plaintiff Barbara M. Brown only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

188. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

189. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

190. Upon information and belief, Plaintiff's Personal Information has already been stolen and misused as she has experienced incidents of fraud and identity theft so far in the form of unauthorized use of her credit card. These actions by unauthorized criminal third parties have

detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

191. Furthermore, Plaintiff has experienced an increase in spam calls related to health services to her cellular device as a result of the Data Breach.

192. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

193. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff has lost time relating to monitoring her accounts and placing a freeze on her credit.

194. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

195. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

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

H. Plaintiff David Pacholczak

197. Plaintiff David Pacholczak is an adult individual and a natural person of New York, residing in Allegany County, where he intends to stay.

198. Plaintiff provided his information to Zoll in connection with a prescribed Zoll medical device.

199. Upon information and belief, Plaintiff David Pacholczak received a notice letter from Defendant Zoll on or about March 10, 2023 informing him of the Data Breach and the exposure of his Private Information.

200. Upon information and belief, the notice letter informed Plaintiff that his PII and PHI were potentially compromised in the Data Breach.

201. Plaintiff David Pacholczak is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

202. Plaintiff David Pacholczak only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

203. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

204. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

205. Upon information and belief, Plaintiff's Personal Information has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of fraudulent and unauthorized use of his debit card. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

206. Furthermore, Plaintiff has experienced an increase of spam phone calls as a result of the Data Breach.

207. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

208. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff has suffered expenses relating to driving to and from the bank to sort out the fraudulent charges discovered on his debit account, as well as time spent speaking with institutions over the phone to resolve late payments, and requesting late charges be reversed, as a result of the Data Breach.

209. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring

his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

210. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety as Plaintiff lives on a fixed monthly income. Plaintiff is retired, has health issues, only receives social security benefits, and is continually worried about how he will pay his expenses if his money is stolen through fraudulent activity.

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

I. Plaintiff Patricia McMahon

212. Plaintiff McMahon is an adult individual and a natural person of Berwyn, Illinois, residing in Cook County, where she intends to stay.

213. Plaintiff gave her information to Zoll in connection with a prescribed Zoll cardiac monitoring device.

214. Plaintiff McMahon received a notice letter from Defendant Zoll dated March 10, 2023, informing her of the Data Breach and the exposure of her Private Information.

215. The notice letter informed Plaintiff that her name, address, Social Security number, and date of birth was potentially compromised in the Data Breach, along with information regarding her status as a user of a Zoll medical device.

216. Plaintiff McMahon is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents.

Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

217. Plaintiff McMahon only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

218. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

219. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

220. Plaintiff has experienced a marked increase in the amount of spam calls (around ten per day) and text messages she has been receiving as a result of the Data Breach, and also received notice of an inaccurate charge to her Medicare account for a catheter, a device which she does not have and has never been prescribed.

221. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

222. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff spends roughly an hour every week reviewing her financial statements, bank accounts, and credit record to ensure that there is no fraud and there are no attempts at identity theft.

223. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

224. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety to such an extent that she has consulted with a therapist regarding these feelings.

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

J. Plaintiff Evan Weese

226. Plaintiff Weese is an adult individual and a natural person of Texas, residing in Bastrop County, where he intends to stay.

227. Plaintiff provided his information to Zoll as a condition of his employment.

228. Plaintiff Weese received a notice letter from Defendant Zoll dated March 10, 2023 informing him of the Data Breach and the exposure of his Private Information.

229. The notice letter informed Plaintiff that his name, address, and his Social Security number was potentially compromised in the Data Breach.

230. Plaintiff Weese is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

231. Plaintiff Weese only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

232. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

233. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

234. Furthermore, Plaintiff has received several notifications that his Private Information has been found on the dark web, and notifications from his financial institutions regarding several attempts at fraudulent transactions as a result of the Data Breach.

235. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

236. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff has already spent several hours responding to and mitigating the damage and risk created by the Data Breach, including time spent reviewing his financial statements and credit history, changing passwords, and communicating with his bank regarding fraud notifications.

237. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

238. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

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

Plaintiffs and the Class Face Significant Risk of Present and Continuing Identity Theft

240. Plaintiffs and Class Members suffered injury from the misuse of their PII and PHI that can be directly traced to Defendant.

241. The ramifications of Defendant's failure to keep Plaintiffs' and the Class's PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license

number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

242. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[21]

243. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiffs and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII and PHI is used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII and PHI; and

[21] Anne Saita, *More Than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report*, ThreatPost (Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/.

h. The continued risk to their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII and PHI in their possession.

244. Stolen PII and PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII and PHI can be worth up to $1,000.00 depending on the type of information obtained.[22]

245. The value of Plaintiffs' and the Class's Private Information on the black market is considerable. Stolen PII and PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

246. It can take victims years to spot or identify PII and PHI theft, giving criminals plenty of time to milk that information for cash.

247. One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.[23]

---

[22] Brian Stack, *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/.

[23] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SEC. (Sep. 18, 2014), https://krebsonsecurity.com/tag/fullz/.

248. Cyber-criminals can cross-reference two sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

249. The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII and PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

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

251. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiffs and the Class that their PII and PHI had been stolen.

252. 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.

253. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII and PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

254. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[24]

255. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[25] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted

[24] *Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[25] *Start With Security, A Guide for Business*, FED. TRADE COMM'N (JUNE 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[26]

256. According to the FTC, unauthorized PII and PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[27] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTCA.

257. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and

[26] *Id.*
[27] *See Taking Charge, What to Do If Your Identity is Stolen*, FED. TRADE COMM'N, at 3 (2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen.

block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Defendant thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII and PHI.

258. The healthcare industry has "emerged as a primary target [for data breaches] because [it sits] on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, ha[s] so much monetizable information stored in their data centers."[28]

259. Charged with handling highly sensitive PII and PHI including healthcare information, financial information, and insurance information, Defendant knew or should have known the importance of safeguarding the PII and PHI that was entrusted to it. Defendant also knew or should have known of the foreseeable consequences if its data security systems were breached. Defendant nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

260. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII and PHI of Plaintiffs and over 1 million members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

261. Plaintiffs and Class Members face substantial risk of being targeted for future

[28] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), https://bit.ly/3x6fz08.

phishing, data intrusion, and other illegal schemes based on Plaintiffs' and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

262. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

263. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyberthieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

264. Plaintiffs and Class Members were also damaged vis-à-vis benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiffs and Class Members paid to Defendants and/or Defendants' healthcare partners was intended to be used by Defendants to fund adequate security of their computer system(s) and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to.

265. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

266. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiffs and Class Members will continue to be at present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

267. Plaintiffs and Class Members have a continuing interest in ensuring that their

Private Information, which, upon information and belief, remains backed up in Zoll's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

268. Plaintiffs bring this class action individually on behalf of themselves and on behalf of all members of the following Classes of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. Plaintiffs seek certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3) of the following Nationwide Class and state subclasses (together the "Classes"):

Nationwide Class

All persons residing in the United States whose Private Information was impacted by the Data Breach—including all who were sent a notice of the Data Breach.

Florida Consumer Subclass

All customers of Zoll residing in the state of Florida whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

Kansas Consumer Subclass

All customers of Zoll residing in the state of Kansas whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

New York Consumer Subclass

All customers of Zoll residing in the state of New York whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

Pennsylvania Consumer Subclass

All customers of Zoll residing in the state of Pennsylvania whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

Illinois Consumer Subclass

All customers of Zoll residing in the state of Illinois whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

Employee Subclass

All current and former employees of Zoll residing in the United States whose Private Information was compromised in the Data Breach, including all who were sent notice of the Data Breach.

269. The Classes defined above are readily ascertainable from information in Defendant's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

270. Excluded from the Classes are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or their parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

271. Plaintiffs reserve the right to amend or modify the Class definitions as this case progresses.

272. Plaintiffs satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

273. **Numerosity**. Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on

information and belief, the Classes consist of the approximately one million individuals whose PII and PHI were compromised by Defendant's Data Breach.

274. **Commonality**. There are many questions of law and fact common to the Classes. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII and PHI;

b. If Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. If Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d. If Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. If Defendant owed a duty to Class Members to safeguard their PII and PHI;

f. If Defendant breached its duty to Class Members to safeguard their PII and PHI;

g. If Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. If Defendant should have discovered the Data Breach earlier;

i. If Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

j. If Defendant's delay in informing Plaintiffs and Class Members of the Data Breach was unreasonable;

k. If Defendant's method of informing Plaintiffs and Class Members of the Data Breach was unreasonable;

l. If Defendant's conduct was negligent;

m. If Plaintiffs and Class Members were injured as a proximate cause or result of the Data Breach;

n. If Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

o. If Defendant breached implied contracts with Plaintiffs and Class Members;

p. If Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

q. If Defendant failed to provide notice of the Data Breach in a timely manner, and;

r. If Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

275. **Typicality**. Plaintiffs' claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, Plaintiffs and Class Members were subjected to Defendant's uniformly illegal and impermissible conduct.

276. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Classes. Plaintiffs' counsel are competent and

experienced in litigating complex class actions. Plaintiffs have no interests that conflict with, or are antagonistic to, those of the Classes.

277. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully exposed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

278. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

279. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

280. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

281. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above.

282. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

283. Plaintiffs re-allege and incorporate by reference paragraphs 1 to 267 of the Consolidated Complaint as if fully set forth herein.

284. Zoll required Plaintiffs and Class Members to provide Defendant with Private Information in order to receive Defendant's products and services.

285. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Zoll owed a duty of care to use reasonable means to secure and safeguard their computer system—and Plaintiffs' and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes so they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

286. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant held vast amounts of PII and PHI, it was inevitable that unauthorized individuals would at some point try to access Defendant's databases of PII and PHI.

287. After all, Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiffs and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the PII and PHI entrusted to them.

288. Defendant owed a duty of care to Plaintiffs 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 PII and PHI.

289. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and Class Members, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

290. Defendant failed to take appropriate measures to protect the PII and PHI of Plaintiffs and the Class. Defendant is morally culpable, given the prominence of security breaches in the healthcare industry. Any purported safeguards that Defendant had in place were wholly inadequate.

291. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' PII and PHI by failing to adopt, implement, and

maintain adequate security measures to safeguard that information, despite known data breaches in the healthcare industry, and allowing unauthorized access to Plaintiffs' and the other Class Members' PII and PHI.

292. The failure of Defendant to comply with industry and federal regulations evinces Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII and PHI.

293. But for Defendant's wrongful and negligent breach of their duties to Plaintiffs and the Class, Private Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII and PHI of Plaintiffs and the Class and all resulting damages.

294. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' PII and PHI. Defendant knew or should have known that their systems and technologies for processing and securing the PII and PHI of Plaintiffs and the Class had security vulnerabilities.

295. As a result of this misconduct by Defendant, the PII, PHI, and other sensitive information of Plaintiffs and the Classes was compromised, placing them at a greater risk of identity theft and their PII and PHI being disclosed to third parties without the consent of Plaintiff and the Class.

296. As a direct and proximate result of Zoll's negligence, Plaintiffs 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 Zoll's possession and is subject to further unauthorized disclosures so long as Zoll 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 Zoll'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.

297. As a direct and proximate result of Zoll's negligence, Plaintiffs 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.

298. Zoll's negligent conduct is ongoing, in that it still possesses Plaintiffs' and Class Members' Private Information in an unsafe and insecure manner.

299. Plaintiffs and Class Members are entitled to injunctive relief requiring Zoll 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.

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class)

300. Plaintiffs re-allege and incorporate by reference paragraphs 1 to 267 of the Complaint as if fully set forth herein.

301. Zoll had had duties arising under HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and the FTC Act to protect Plaintiffs' and Class Members' Private Information.

302. Zoll breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information. The specific negligent acts and omissions committed by Zoll 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 former employees' 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.

303. Zoll'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*.

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

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

306. 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 Plaintiffs and the Class.

307. Zoll breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

308. Plaintiffs and Class Members were foreseeable victims of Zoll's violations of HIPAA, HITECH, and the FTC Act. Zoll knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Class Members' Private Information would cause damage to Plaintiffs and the Class.

309. As a direct and proximate result of Zoll's negligence *per se*, Plaintiffs 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 Zoll's possession and is subject to further unauthorized disclosures so long as Zoll fails to undertake appropriate and adequate measures to protect the Private Information.

310. As a direct and proximate result of Zoll's negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury, including, but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

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

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

312. Plaintiffs re-allege and incorporate by reference paragraphs 1 to 267 of the Complaint as if fully set forth herein.

313. Plaintiffs and Class Members conferred a benefit on Defendant by entrusting their Private Information to Zoll from which Zoll derived profits.

314. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide adequate security.

315. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

316. Defendant acquired the PII and PHI through inequitable means in that Defendant failed to disclose the inadequate security practices, previously alleged, and failed to maintain adequate data security.

317. If Plaintiffs and Class Members knew that Defendant had not secured their PII and PHI, they would not have agreed to disclose their data to Defendant.

318. Plaintiffs and Class Members have no adequate remedy at law.

319. As a direct and direct an proximate result of Zoll's conduct, Plaintiffs 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 Zoll's possession and is subject to further unauthorized disclosures or further entrustment to inadequate third party vendors so long as Zoll 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 Zoll'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.

320. Plaintiffs and Class Members are entitled to restitution and/or damages from Zoll and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by

Zoll 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 Plaintiffs and Class Members may seek restitution or compensation.

321. Plaintiffs and Class Members may not have an adequate remedy at law against Zoll, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Nationwide Class)

322. Plaintiffs re-allege and incorporate by reference paragraphs 1 to 267 of the Complaint as if fully set forth herein.

323. A relationship existed between Plaintiffs, the Class Members, and Defendant, which arose from Defendant's acceptance of Plaintiffs' and the Class Members' PII and PHI and Defendant's representations of its commitment to protect said PII and PHI.

324. Zoll became the guardian of Plaintiffs' and Class Members' Private Information. Zoll became a fiduciary, created by its undertaking and guardianship of Plaintiffs' and Class Members' Private Information, to act primarily for their benefit. This duty included the obligation to safeguard Plaintiffs' and Class Members' Private Information and to timely detect and notify Plaintiffs and Class Members in the event of a data breach.

325. The interests of public policy mandates that a fiduciary duty is imputed given Defendant's acceptance of Plaintiffs' and the Class Members' Private Information and Defendant's representations of its commitment to protect said Private Information.

326. Defendant breached the fiduciary duty that it owed to Plaintiffs and Class Members because Defendant failed to act with the utmost good faith, fairness, honesty, the highest degree of loyalty, ultimately failed to protect the Private Information of Plaintiffs and Class Members.

327. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiffs and Class Members.

328. But for Defendant's breach of fiduciary duty, the damage to Plaintiffs and Class Members would not have occurred.

329. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiffs and Class Members.

330. As a direct and proximate result of Zoll's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered or will suffer concrete injury, including, but not limited to: (a) actual identity theft; (b) the loss of the opportunity to determine how and when their Private Information is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; € lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Zoll's possession and is subject to further unauthorized disclosures so long as Zoll fails to undertake appropriate and adequate measures to protect Private Information in its continued possession and ensure that it retains vendors who adequately protect Private Information; (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, and repair the impact of the Private Information compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (h) nominal damages.

331. As a direct and proximate result of Zoll's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

332. Plaintiffs re-allege and incorporate by reference paragraphs 1 to 267 of the Complaint as if fully set forth herein.

333. Through their course of conduct, Defendant, Plaintiffs, and Class Members entered into contracts for the provision of medical equipment or employment, as well as implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

334. Specifically, Plaintiffs entered into a valid and enforceable implied contracts with Defendant when they first applied for or obtained health care devices or employment from Zoll.

335. The valid and enforceable implied contracts to provide health care or employment that Plaintiffs and Class Members entered into with Defendant and/or its healthcare provider-customers include the promise to protect non-public Private Information given to Defendant or that Defendant creates on its own from disclosure.

336. When Plaintiffs and Class Members provided their Private Information to Defendant and/or its healthcare provider-customers in exchange for medical devices or employment, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

337. Defendant and/or its agents solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

338. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

339. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

340. Under the implied contracts, Defendant and/or its healthcare provider-customers promised and were obligated to: (a) provide healthcare equipment or employment to Plaintiffs and Class Members; and (b) protect Plaintiffs' and the Class Members' PII/PHI: provided to obtain such healthcare equipment or employment; and/or created as a result of providing such services. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

341. Both the provision of healthcare equipment or employment and the protection of Plaintiffs' and Class Members' Private Information were material aspects of these implied contracts.

342. The implied contracts for the provision of healthcare equipment or employment–contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's privacy policies.

343. Defendant's express representation memorialize and embody the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

344. Consumers of healthcare and employees value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To Plaintiffs and Class Members, healthcare equipment or employment that do not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant nor its healthcare provider-customers and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

345. A meeting of the minds occurred, as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendant and/or its Agents, and paid for the provided services in exchange for, amongst other things, both the provision of healthcare equipment or employment and the protection of their Private Information.

346. Plaintiffs and Class Members performed their obligations under the contract when they paid for their healthcare equipment or applied employment and provided their Private Information.

347. Defendant materially breached its contractual obligation to protect the non-public Private Information Defendant gathered when the sensitive information was accessed by unauthorized personnel as part of the Data Breach.

348. Defendant materially breached the terms of the implied contracts. Defendant did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and approximately 1 million Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiffs' and the Class Members' Private Information, as set forth above.

349. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

350. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare equipment or employment that were of a diminished value to that described in the contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare services or employment data security protection they paid for and the health care services they received.

351. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare equipment from nor applied for employment with Defendant and/or its affiliated healthcare providers.

352. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the

future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

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

354. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity monitoring to all Class Members.

SIXTH CAUSE OF ACTION
Declaratory Judgment/Injunctive Relief
(On Behalf of Plaintiffs and the Nationwide Class)

355. Plaintiffs re-allege and incorporate by reference paragraphs 1 to 267 of the Complaint as if fully set forth herein.

356. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

357. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Private Information and whether Zoll is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Plaintiffs allege that Zoll's data security measures remain inadequate.

358. Indeed, in December 2023, less than a year after Zoll announced the Data Breach at issue in this Consolidated Amended Complaint, Zoll disclosed yet another cybersecurity incident that exposed the PHI of current and former employees, dependents and beneficiaries.

359. Zoll has characterized the cybersecurity incident as an email phishing attack, targeted at a Zoll employee. The cybersecurity incident involved individuals' names, addresses, Social Security numbers, and protected health information and/or health insurance information.

360. Zoll's December 2023 cybersecurity incident demonstrates the need for injunctive relief for Plaintiffs and Class Members. Zoll has not implemented measures to protect Private Information, leaving Plaintiffs and Class Members without a way of protecting themselves.

361. Plaintiffs continue to suffer injuries as result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

362. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: (a) Zoll owes a legal duty to secure employees' Private Information, and to timely notify impacted individuals of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes, and (b) Zoll continues to breach this legal duty by failing to employ reasonable measures to secure Private Information in its possession.

a. Order Zoll to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Zoll's explicit or implicit contractual obligations and duties of care, Zoll must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. prohibiting Zoll from engaging in the wrongful and unlawful acts alleged herein;

ii. requiring Zoll to protect, including through encryption, all data collected

through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Zoll to delete and purge the Private Information of Plaintiffs and Class Members unless Zoll can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Zoll to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

v. requiring Zoll to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Zoll's systems on a periodic basis;

vi. prohibiting Zoll from maintaining Plaintiffs' and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Zoll to segment data by creating firewalls and access controls so that, if one area of Zoll's network is compromised, hackers cannot gain access to other portions of Zoll's systems;

viii. requiring Zoll to conduct regular database scanning and securing checks;

ix. requiring Zoll to monitor ingress and egress of all network traffic;

x. requiring Zoll to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees'

respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xi. requiring Zoll to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Zoll's policies, programs, and systems for protecting personal identifying information;

xii. requiring Zoll to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Zoll's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Zoll to meaningfully educate all Class Members about the threats that it faces because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

363. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at, or implicating, Zoll. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

364. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Zoll if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Zoll of complying with an injunction by employing

reasonable prospective data security measures is relatively minimal, and Zoll has a pre-existing legal obligation to employ such measures.

365. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Zoll, thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose confidential information would be further compromised.

SEVENTH CAUSE OF ACTION
Florida Deceptive And Unfair Trade Practices Act ("FDUTPA")
Fla. Stat. §§ 501.201 *et seq.*
(On Behalf of Plaintiffs McGilberry, Brown, and the Florida Consumer Subclass)

199. Plaintiffs Randy McGilberry and Barbara Brown (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the allegations contained in paragraphs 1 through 267 above, as if fully set forth herein.

200. Plaintiffs bring this claim on behalf of themselves and the Florida Consumer Subclass.

201. Plaintiffs and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

202. Zoll advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

203. Zoll engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Florida Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and

sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Florida Consumer Subclass Members' Private Information, including by implementing and maintaining security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Consumer Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 45 C.F.R. § 164, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Florida Consumer Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Consumer Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45,

HIPAA, 45 C.F.R. § 164, and Florida's data security statute, F.S.A. § 501.171(2).

204. Zoll's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Zoll's data security and ability to protect the confidentiality of consumers' Private Information.

205. Zoll intended to mislead Plaintiffs and Florida Subclass Members and induce them to rely on its misrepresentations and omissions.

206. Had Zoll disclosed to Plaintiffs and Florida Consumer Subclass Members that its data systems were not secure and, thus, were vulnerable to attack, Zoll would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Zoll was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs and Florida Consumer Subclass Members. Zoll accepted the responsibility of protecting the data but kept the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Florida Consumer Subclass Members acted reasonably in relying on Zoll's misrepresentations and omissions, the truth of which they could not have discovered.

207. As a direct and proximate result of Zoll's unconscionable, unfair, and deceptive acts and practices, Plaintiffs and Florida Consumer Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Zoll's services; loss of the value of access to their Private Information; and the

value of identity protection services made necessary by the Data Breach.

208. Plaintiffs and Florida Consumer Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

EIGTH CAUSE OF ACTION
Kansas Consumer Protection Act
Kan. Stat. Ann. §§ 50-623 *et seq.*
(On Behalf of Plaintiff Gary Becker and the Kansas Consumer Subclass)

209. Plaintiff Gary Becker (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 267 above, as if fully set forth herein.

210. Plaintiff brings this claim on behalf of himself and the Kansas Consumer Subclass.

211. K.S.A. §§ 50-623 *et seq*. is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

212. Plaintiff and Kansas Consumer Subclass Members are "consumers" as defined by K.S.A. § 50-624(b).

213. The acts and practices alleged herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

214. Zoll is a "supplier" as defined by K.S.A. § 50-624(l).

215. Zoll advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

216. Zoll engaged in deceptive and unfair acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Kansas Consumer Class Members'

Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kansas Consumer Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Kansas Consumer Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kansas Consumer Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Kansas Consumer Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not

comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kansas Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b; and

h. Omitting, suppressing, and concealing the material fact that it did not implement and maintain reasonable security and privacy measures to protect Plaintiff's and Kansas Class Members' Private Information, which was a direct and proximate cause of the Data Breach.

217. Zoll's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Zoll's data security and ability to protect the confidentiality of consumers' Private Information.

218. Zoll intended to mislead Plaintiff and Kansas Consumer Class Members and induce them to rely on its misrepresentations and omissions.

219. Had Zoll disclosed to Plaintiff and Kansas Consumer Class Members that its data systems were not secure and, thus, vulnerable to attack, Zoll would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Zoll was trusted with sensitive and valuable Private Information regarding over one million consumers, including Plaintiff and Kansas Class Members. Zoll accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Kansas Class Members acted reasonably in relying on Zoll's misrepresentations and omissions, the truth of which they could not have discovered.

220. Zoll also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Kansas Class to reasonably protect their interests, due to their lack of knowledge (see K.S.A. § 50-627(b)(1)); and

b. Requiring Plaintiff and the Kansas Consumer Subclass to enter into a consumer transaction on terms that Zoll knew were substantially one-sided in favor of Zoll (see K.S.A. § 50- 627(b)(5)).

221. Plaintiff and the Kansas Consumer Subclass had unequal bargaining power with respect to their ability to control the security and confidentiality of their Private Information in Zoll's possession.

222. The above unfair, deceptive, and unconscionable practices and acts by Zoll were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Consumer Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

223. Zoll acted intentionally, knowingly, and maliciously to violate the Kansas's Consumer Protection Act, and recklessly disregarded Plaintiff's and Kansas Consumer Subclass Members' rights.

224. As a direct and proximate result of Zoll's unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Consumer Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Zoll's services; loss of the value of access to their Private Information; and the value of identity protection

services made necessary by the Data Breach.

225. Plaintiff will provide notice of this action to the Attorney General of Kansas. Plaintiff and Kansas Class Members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

NINTH CAUSE OF ACTION
New York General Business Law,
N.Y. Gen. Bus. Law §§ 349 *et seq.*
(On Behalf of Plaintiff Pacholczak and the New York Consumer Subclass)

226. Plaintiff Pacholczak (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the allegations contained in paragraphs 1 through 267 above, as if fully set forth herein.

227. Plaintiff brings this claim on behalf of himself and the New York Consumer Subclass.

228. Zoll engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and New York Consumer Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the

security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164.

229. Zoll's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Private Information.

230. Zoll acted intentionally, knowingly, and maliciously to violate New York's General

Business Law, and recklessly disregarded Plaintiff and New York Consumer Subclass Members' rights.

231. As a direct and proximate result of Zoll's deceptive and unlawful acts and practices, Plaintiff and New York Consumer Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Zoll's products and services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

232. Zoll's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the New Yorkers affected by the Data Breach.

233. The above deceptive and unlawful practices and acts by Zoll caused substantial injury to Plaintiff and New York Consumer Subclass Members that they could not reasonably avoid.

234. Plaintiff and New York Consumer Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

TENTH CAUSE OF ACTION
Pennsylvania Unfair Trade Practices and Consumer Protection Law,
73 P.S. § 201-3
(On Behalf of Plaintiff Bendriss and the Pennsylvania Consumer Subclass)

235. Plaintiff Bendriss for the purposes of this count, "Plaintiff") realleges and incorporate by reference the allegations contained in paragraphs 1 through 267 above, as if fully set forth herein.

236. Plaintiff brings this claim on behalf of herself and the Pennsylvania Subclass.

237. Zoll engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of 73 P.S. § 201-3, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Pennsylvania Consumer Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Pennsylvania Consumer Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Pennsylvania Consumer Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. §

45, and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Pennsylvania Consumer Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164.

238. Zoll's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Private Information.

239. Zoll acted intentionally, knowingly, and maliciously to violate Pennsylvania law and recklessly disregarded Plaintiff's and Pennsylvania Consumer Subclass Members' rights.

240. Plaintiff and Pennsylvania Consumer Subclass Members justifiably relied on the above-mentioned misrepresentations.

241. Plaintiff and Pennsylvania Consumer Subclass Members would not have engaged in business with Zoll or provided Zoll with their Private Information but for Zoll's misrepresentations regarding its protection of that Private Information.

242. As a direct and proximate result of Zoll's deceptive and unlawful acts and practices, Plaintiff and Pennsylvania Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to

monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Zoll's products and services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

243. Zoll's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the Pennsylvanians affected by the Data Breach.

244. The above deceptive and unlawful practices and acts by Zoll caused substantial injury to Plaintiff and Pennsylvania Consumer Subclass Members that they could not reasonably avoid.

245. Plaintiff and Pennsylvania Consumer Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

ELEVENTH CAUSE OF ACTION
Illinois Consumer Fraud and Deceptive Business Practices Act,
815 ILCS 505/1
(On Behalf of Plaintiff Priddy, Plaintiff McMahon and the Illinois Consumer Subclass)

246. Plaintiffs Priddy and McMahon (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the allegations contained in paragraphs 1 through 267 above, as if fully set forth herein.

247. Plaintiffs bring this claim on behalf of themselves and the Illinois Consumer Subclass.

248. Plaintiffs are "consumers" pursuant to 815 ILCS 505/1(e).

249. Zoll engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of 815 ILCS 505 et seq, including:

a. Failing to implement and maintain reasonable security and privacy

measures to protect Plaintiffs' and Illinois Consumer Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Consumer Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Consumer Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Illinois Consumer Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not

comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Consumer Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164.

250. Zoll's representations and omissions were material because Zoll knew the representations and omissions were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Private Information.

251. Zoll acted intentionally, knowingly, and maliciously to violate Illinois law and recklessly disregarded Plaintiffs' and Illinois Consumer Subclass Members' rights.

252. Plaintiffs and Illinois Consumer Subclass Members justifiably relied on the above-mentioned misrepresentations.

253. Plaintiffs and Illinois Consumer Subclass Members would not have engaged in business with Zoll nor provided Zoll with their Private Information but for Zoll's misrepresentations regarding its protection of that Private Information.

254. As a direct and proximate result of Zoll's deceptive and unlawful acts and practices, Plaintiffs and Illinois Consumer Subclass Members have suffered and will continue to suffer actual damages, ascertainable losses of money or property, and monetary and nonmonetary damages, as described herein, including but not limited to: fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Zoll's products and services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

255. Zoll's deceptive and unlawful acts and practices complained of herein affected the

public interest and consumers at large, including the Illinois affected by the Data Breach.

256. The above deceptive and unlawful practices and acts by Zoll caused substantial injury to Plaintiffs and Illinois Consumer Subclass Members that they could not reasonably avoid.

257. Plaintiffs and Illinois Consumer Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs, on behalf of themselves and all others similarly situated, request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiffs as Class Representatives;

B. A mandatory injunction directing Defendant to adequately safeguard the PII and PHI of Plaintiffs and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete and purge the PII and PHI of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive

Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' PII and PHI;

v. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

vi. prohibiting Defendant from maintaining Plaintiffs' and Class Members' PII and PHI on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to monitor ingress and egress of all network traffic;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII and PHI, as well as protecting the PII and PHI of Plaintiffs and Class Members;

xi. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems

for protecting personal identifying information;

xii. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII and PHI to unauthorized persons;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII and PHI;

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiffs and the Class leave to amend this Complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury for any and all issues in this action so triable as of right.

Dated: February 26, 2024

Respectfully Submitted,

/s/ Jean S. Martin
JEAN S. MARTIN
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 559-4908
jeanmartin@ForThePeople.com

Interim Lead Counsel for Plaintiffs and the Class

CERTIFICATE OF SERVICE

I hereby certify that on February 26, 2024, I electronically filed Plaintiffs' Consolidated Class Action Complaint by using the CM/ECF system, which will send a notice of electronic filing to all counsel of record.

s/ Jean S. Martin
Jean S. Martin

EXHIBIT 1

ZOLL
an Asahi Kasei company
269 Mill Road
Chelmsford, MA 01824

March 10, 2023

J1341-L02-0000002 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L02 US HIPAA + STATE LAW PATIENT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Dear Sample A. Sample:

ZOLL recently learned of a data security incident that may have affected some of your protected health information. We are writing to notify you of this incident as well as provide you with information on the actions that ZOLL has taken in response, resources available to you, and steps you can take to protect yourself.

Notice of Data Security Incident
ZOLL recently experienced a cybersecurity incident that may have resulted in the disclosure of some of your protected health information. Based on our investigation, we have no indication that any of your information has been misused. ZOLL is notifying all individuals whose information was affected.

What Happened?
On January 28, 2023, we detected unusual activity on our internal network, and we promptly took steps to mitigate the incident. We consulted with third-party cybersecurity experts to assist with our response to the incident, and we notified law enforcement. We determined that your information may have been affected on or about February 2, 2023. Our investigation into the incident is ongoing.

What Information Was Involved?
Information that may have been disclosed includes your name, address, date of birth, and Social Security number. It may also be inferred that you used or were considered for use of a ZOLL product.

What Measures Have We Taken to Remedy the Situation?
We consulted with third-party cybersecurity experts to assist with our response to and remediation of the incident, and we notified law enforcement and federal and state regulatory agencies as required by law.

Additionally, to help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 24 months.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** May 31, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/pluscreditlock
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **800-459-5782** by May 31, 2023. Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

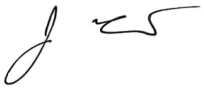
What You Can Do

It is important to be careful when receiving emails or other communications from unknown individuals, including any communications with your medical details. You may also take advantage of the complimentary identity protection services being offered.

For More Information

We sincerely regret any inconvenience or concern this incident may cause you. If you have any questions or need any additional information, please do not hesitate to call **800-459-5782** toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number **B086101.**

Sincerely,



Jonathan A. Rennert, Chief Executive Officer

This is a legal notice that is sent to all individuals whose information was potentially affected, which is why you are receiving this letter, even if you never used or are no longer using ZOLL products.

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®	**Experian**	**TransUnion®**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com/personal/credit-report-services	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's

credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

If you are a resident of the **District of Columbia**, you may wish to contact the Office of the Attorney General, Office of Consumer Protection at 400 6th Street, NW
Washington, DC 20001, by phone at 202-442-9828 or by email at consumer.protection@dc.gov. You can also visit the Office of Consumer Protection's website at https://oag.dc.gov/consumer-protection for more information.

If you are a resident of **Iowa**, you may wish to report suspected incidents of identity theft to local law enforcement or the Attorney General, Consumer Protection Division, at Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, by phone at 515-281-5926 or 888-777-4590, or by email at consumer@ag.iowa.gov. You can also visit the Consumer Protection Division website at https://www.iowaattorneygeneral.gov/for-consumers for more information.

If you are a resident of **Maryland**, you may wish to contact the Attorney General, Consumer Protection Division, for more information at 200 St. Paul Place, Baltimore, MD 21202, by telephone at 410-528-8662 or 888-743-0023, or by email at Consumer@oag.state.md.us.
You can also visit the Consumer Protection Division website at https://www.marylandattorneygeneral.gov/Pages/CPD/default.aspx for more information.

If you are a resident of **Massachusetts**, please note that you have the right to file or obtain a police report related to this incident.

If you are a resident of **New Mexico**, please note your rights under the Fair Credit Reporting Act, which can be viewed here https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

If you are a resident of **New York**, you may wish to contact the Attorney General's Office at The Capitol, Albany, NY 12224-0341, or by telephone at 800-771-7755 or 800-788-9898. You may also contact the Department of State, Consumer Protection Division at 800-697-1220 or to visit https://www.dos.ny.gov/consumerprotection/ for more information.

If you are a resident of **North Carolina**, you may wish to contact the Attorney General's Office at 9001 Mail Service Center Raleigh, NC 27699-9001, or by telephone at 919-716-6000. You can also find more information from the Consumer Protection Division by visiting https://ncdoj.gov/protecting-consumers/.

If you are a resident of **Oregon**, you may wish to contact the Attorney General's Consumer Protection Division by email at help@oregonconsumer.gov or by telephone at 877-877-9392. You may also visit https://www.doj.state.or.us/consumer-protection/ for more information.

If you are a resident of **Puerto Rico**, please note that there were 1,301 affected patients residing in Puerto Rico.

If you are a resident of **Rhode Island**, you may wish to contact the Attorney General's Office, Consumer Protection, at 150 South Main Street Providence, RI 02903 or by telephone at 401-274-4400. You may also visit https://riag.ri.gov/consumerprotection for more information. You also have the right to file or obtain a police report. Please not that there were 1,767 affected patients residing in Rhode Island.

If you are a resident of **Texas**, please note that there were 105,306 affected patients residing in Texas.

Remember to remain vigilant in reviewing your account statements, monitoring your free credit reports, and for incidents of fraud or identity theft.