STATE OF RHODE ISLAND
KENT, S.C.

SUPERIOR COURT

JEANNETTE LAVOIE-SORIA, REBECCA REILLY, FREDERICK WHELAN, PATRICIA ROBINSON and ARIA E. DIMEO, *individually and on behalf of all others similarly situated*, Plaintiffs,	)	
v.	)	C.A. No.: KC-2024-1172
ORTHOPEDICS RHODE ISLAND, INC. Defendant.	)	

AMENDED CLASS ACTION COMPLAINT FOR DAMAGES

Plaintiffs Jeannette Lavoie-Soria, Rebecca Reilly, Frederick Whelan, Patricia Robinson and Aria E. DiMeo ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this action against Defendant Orthopedics Rhode Island, Inc. ("Defendant"), and allege, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Defendant is an orthopedic care provider that specializes in helping its patients recover from injuries.[1] Defendant collects a significant amount of data including personally identifiable information ("PII") including names, addresses, dates of birth, billing and claims information, health insurance claims information, and medical information including diagnosis, medications, test results, x-ray images and other treatment information ("PHI") (collectively, "Private Information").

[1] https://www.orthopedicsri.com/overview/ (last visited January 21, 2025).

2. According to the Notice of Data Security Event that Defendant posted on its own website, between September 4, 2024 and September 8, 2024, an unauthorized party accessed Defendant's computer systems ("Data Breach").[2] As a result of this network access, the Private Information of Plaintiffs and Class Members was compromised due to Defendant's complete failure to protect the data it collects and stores on its network and its unwillingness to act lawfully after the Data Breach occurred.

3. Against this backdrop, Plaintiffs bring this action on behalf of all similarly situated persons whose Private Information was compromised as a result of Defendant's failure: (i) to adequately protect the Private Information of Plaintiffs and Class Members; (ii) to forewarn Plaintiffs and Class Members of its inadequate information security practices; and (iii) to avoid continuing to collect, retain, and use the Private Information of Plaintiffs and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

4. Plaintiffs and Class Members have suffered injuries as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of their Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and, significantly, (iv) the continued and certainly an increased risk to their Private Information.

[2] https://www.orthopedicsri.com/notices/ (last visited January 22, 2025).

II. PARTIES

Plaintiff Jeannette Lavoie-Soria

5. Plaintiff Jeannette Lavoie-Soria is a citizen and resident of West Warwick, RI and a former patient of Defendant.

Plaintiff Rebecca Reilly

6. Plaintiff Rebecca Reilly is a citizen and resident of Jamestown, RI and a former patient of Defendant.

Plaintiff Frederick Whelan

7. Plaintiff Frederick Whelan is a citizen and resident of Seekonk, MA and a former patient of Defendant.

Plaintiff Patricia Robinson

8. Plaintiff Patricia Robinson is a citizen and resident of Coventry, RI, and a former patient of Defendant.

Plaintiff Aria E. DiMeo

9. Plaintiff Aria E. DiMeo is a citizen and resident of Providence, RI and a patient of Defendant.

Defendant Orthopedics Rhode Island, Inc.

10. Defendant is a Rhode Island corporation with its headquarters and principal place of business located at 200 Crossings Boulevard, Suite 310, Warwick, RI 02886.

11. On or about November 6, 2024, Defendant posted a Notice of Data Security Event on its website. *See* https://www.orthopedicsri.com/notices/ (last visited January 22, 2025).

III. JURISDICTION AND VENUE

12. Jurisdiction and venue are proper in this County because Defendant is located and conducts business from its offices in this County, and because Defendant's misconduct, which is the basis of this action, occurred in this County.

13. Venue is proper in this Court pursuant to RI Gen Laws § 9-4-3 because Defendant resides in Kent County.

IV. GENERAL ALLEGATIONS

Defendant's Business

14. Defendant is an orthopedic care provider that operates eight (8) clinics and offices throughout Rhode Island.

15. In order to conduct its business, Defendant requires that its patients provide it with their Private Information.

16. Defendant collects and stores Plaintiffs' and the proposed Class Members' Private Information on its computer systems, including but not limited to names, addresses, dates of birth, billing and claims information, health insurance claims information, and medical information including diagnosis, medications, test results, x-ray images and other treatment information.

17. When Defendant collects this Private Information, it promises to use reasonable care to protect and safeguard the Private Information from unauthorized disclosure.

18. Defendant represented to its patients that they would take adequate measures to safeguard their Private Information, and Plaintiffs and members of the proposed Class relied on Defendant's representations when they agreed to provide their Private Information to Defendant.

19. Despite their alleged commitments to securing sensitive patient data, Defendant did not follow industry standard practices in securing patients' Private Information and failed to

protect the Private Information of Plaintiffs and the proposed Class Members from unauthorized disclosure in the Data Breach.

Obligations of Defendant

20. Plaintiffs and Class Members relied on Defendant's promises to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their Private Information.

21. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from involuntary disclosure to third parties.

22. Defendant recognizes these duties, declaring in its HIPAA Omnibus Notice of Privacy Practices (referred to herein as Defendant's "Privacy Policy") that:

a. "This Notice of Privacy Practices describes how we, our Business Associates and their subcontractors, may use and disclose your Protected Health Information (PHI) to carry out Treatment, Payment or Health Care Operations (TPO) and for other purposes that are permitted or required by law. It also describes your rights to access and control your Protected Health Information.

b. "Some examples of Protected Health Information include information about your past, present or future physical or mental health condition, genetic information, or information about your health care benefits under an insurance plan, each when combined with identifying information such as your name, address, social security number or phone number."

c. "You have the right to be notified within sixty (60) days of the discovery of a breach of your unsecured protected health information if there is more than a low probability the information has been compromised."

23. The healthcare sector is a favored target by cybercriminals, yet recent studies, including one by the Massachusetts Institute of Technology, found medical centers lagged behind other businesses in safeguarding their computer systems. A Tenable study analyzing healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in nearly 93% of the breaches."

24. Despite recognizing its duty to do so, on information and belief, Defendant did not and, upon information and belief, still has not implemented reasonably necessary cybersecurity safeguards or policies to protect its patients' Private Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Defendant left significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' Private Information.

25. As a result of Defendant's failure to implement and follow basic security procedures, the Private Information of Plaintiffs and Class Members was more likely than not accessed, disclosed, and/or acquired and is now in the hands of criminals.

26. Once information is placed onto the internet, it is virtually impossible to remove. Plaintiffs and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiffs and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves from identity theft due to Defendant's failures.

27. Additionally, as a result of Defendant's failure to follow industry standard security procedures, Plaintiffs and Class Members received a diminished value for the services Defendant was to provide.

28. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access, intrusion, and/or acquisition.

29. Moreover, Defendant now put the burden squarely on Plaintiffs and Class Members to enroll in the credit monitoring services, among other steps Plaintiffs and Class Members must take to protect themselves. Time is a compensable and extremely 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.

30. 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; leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'" Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, patients 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.

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

The Data Breach

32. On or about November 6, 2024, Defendant posted notice of the Data Breach on its website, and stated in relevant part:

> November 6, 2024 – Orthopedics Rhode Island, Inc. ("Ortho RI") recently discovered a data event that may have impacted the privacy of information related to certain individuals. This notice provides details of the event, Ortho RI's response, and steps individuals may take to help protect their personal information should they feel it is appropriate to do so.
>
> On September 7, 2024, Ortho RI identified suspicious activity on its network, and immediately took steps to secure our systems and initiated an investigation into the nature and scope of the activity. The investigation determined that Ortho RI's network was subject to a data security event between September 4, 2024, and September 8, 2024. While Ortho RI has no evidence of misuse of the any information or fraudulent activity as a result of this event, it is notifying individuals potentially impacted out of an abundance of caution.
>
> The types of information that may have been present on the impacted systems includes name, address, date of birth, billing and claims information, health insurance claims information, and medical information including diagnosis, medications, test results, x-ray images and other treatment information. Please note that the specific type of information may vary for each individual.[3]

33. Alarmingly, Defendant admitted that "certain files were *acquired* by an unknown actor."[4]

34. In other words, Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain and exfiltrate files containing a treasure trove of its patients' Private Information.

[3] *See* https://www.orthopedicsri.com/notices/ (last visited January 22, 2025).

[4] Defendant's Breach Notice.

35. And yet, Defendant waited until December 6, 2024, before it began notifying the class—a full *90 days* after it discovered the Data Breach.[5]

36. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

37. And when Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

a. "We encourage you to remain vigilant against events of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."[6]

b. "We also encourage you to review the enclosed *Steps You Can Take to Help Protect Your Personal Information*."[7]

38. Since the Data Breach, Defendant states it is "reviewing and enhancing its existing policies and procedures to reduce the likelihood of a similar event in the future."[8]

39. But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

40. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

---

[5] *Id.*

[6] *Id*.

[7] *Id*.

[8] *Id*.

41. Defendant has done little to remedy its Data Breach. It suggested victims "monitor" their accounts and provided publicly available information regarding how to put a "credit freeze" on one's credit report.[9] But upon information and belief, such information is wholly insufficient to compensate Plaintiff and Class Members for the injuries that Defendant inflicted upon them.

42. Because of Defendant's Data Breach, the sensitive PII/PHI of Plaintiffs and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class Members.

43. Indeed, on November 12, 2024, Hackmanac, a cybersecurity firm that compiles a weekly list of cyberattacks[10], listed Defendant as an entity that had experienced a cyberattack.[11]

44. Thus, on information and belief, Plaintiffs' and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

45. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing their Private Information to be exposed.

46. To prevent and detect network server intrusions, Defendant could and should have implemented, as recommended by the United States Government, the following non-exhaustive list of measures:

- Utilize strict access controls, remove backdoor connections, and limit virtual private networks.
- Maintain adequate file system and boot management, stay updated with vendor-supported software, and verify software and configuration settings.
- Use centralized servers, configure authentication, authorization, and accounting, implement the principle of 'least privilege.

[9] *Id.*

[10] *See About Us*, HACKMANAC, https://hackmanac.com/about-us (last visited Jan. 22, 2025).

[11] *See HACK TUESDAY WEEK 06 - 12 NOVEMBER 2024*, HACKMANAC, https://hackmanac.com/news/hack-tuesday-week-06-12-november-2024 (last visited Jan. 22, 2025).

- Incorporate specific usernames and account settings, change default passwords, eliminate unnecessary accounts, and store passwords with safe algorithms.
- Configure logging and centralized remote log servers, obtain necessary log information, and synchronize clocks.
- Refrain from using cleartext services, verify appropriate encryption strength, use secure protocols, restrict access to services, and turn off unneeded network services.
- Turn off Internet Protocol service routing and turn on routing authentication.
- Enable port security and disable default virtual local area networks, unused ports, port monitoring, and proxy Address Resolution Protocol.

47. Given that Defendant was storing the Private Information of the patients it was providing services to, Defendant could and should have implemented all the above measures to prevent and detect network server intrusions.

48. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its patients' Private Information.

49. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the recommended list of measures to prevent network server intrusions, resulting in the Data Breach and the exposure of the Private Information of individuals like Plaintiffs and Class Members.

The Data Breach Was Foreseeable Because the Healthcare Sector is Particularly Vulnerable to Cyber Attacks.

50. Defendant was on notice that companies in the healthcare industry are targets for data breaches.

51. Defendant was on further notice regarding the increased risks of inadequate cybersecurity. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were

"advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain Private Information." *See* https://archives.fbi.gov/archives/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism. The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." *Id.*

52. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year. In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.

53. That trend continues. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

54. In February 2022, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic rise in cyberattacks, urging facilities to shore up their cyber defenses. Indeed, just days before, HHS's cybersecurity arm issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.

55. In light of recent high profile data breaches at other healthcare partner and provider companies, Defendant knew or should have known that its electronic records and patients' Private Information would be targeted by cybercriminals.

56. In the context of data breaches, healthcare is "by far the most affected industry sector." 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 Private Information. A Tenable study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in *nearly 93% of the breaches*."

57. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)." *See* https://www.reuters.com/article/technology/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U/.

58. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.

59. The healthcare sector consistently reports one of the highest number of breaches among all measured sectors, with the highest rate of exposure per breach. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30

percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.

60. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit 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, have so much monetizable information stored in their data centers."

Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' Personal Information.

61. In the course of its regular business operations, Defendant acquired, collected, and stored Plaintiffs' and Class Members' Private Information.

62. As a condition of its relationship with Plaintiffs and Class Members, Defendant required that Plaintiffs and Class Members entrust Defendant with highly confidential Private Information.

63. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

64. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

65. Yet, despite the prevalence of public announcements of these data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiffs' and Class Members' Private Information from being compromised.

Securing Private Information and Preventing Breaches

66. Defendant could have prevented this Data Breach by properly securing its networks and encrypting the Private Information of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially decade-old data from former patients. Further, Defendant could have prevented this Data Breach by properly overseeing its patients' Private Information – including assuring that Private Information collected was properly protected and maintained and adhered to a reasonable deletion schedule.

67. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

68. Indeed, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

69. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

70. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

71. The Personal Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data breaches from $900 to $4,500.

72. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

73. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of

misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

74. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

75. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name and date of birth.

76. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."

77. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

78. Indeed, cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class Members' Private Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and

combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

79. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

80. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/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 Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

81. The Private Information of Plaintiffs and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the Private Information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

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

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

83. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the

foreseeable consequences that would occur if the Private Information was compromised, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members a result.

84. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Personal Information.

85. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on its systems and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

86. To date, Defendant has suggested obtaining a credit report or placing a freeze on credit, but Defendant has offered nothing to the victims.

87. Further, there is a market for Plaintiffs' and Class Members PHI, and the stolen PHI has inherent value.

88. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

89. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."

90. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Defendant's Conduct Violates the Rules and Regulations of HIPAA and HITECH.

91. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients, or in this case, patients' medical information safe. 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.

92. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Private Information is properly maintained.

93. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS has subsequently

promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

94. Defendant is a covered entity pursuant to HIPAA. *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. See 45 C.F.R. Part 160 and Part 164, Subparts A through E.

95. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

96. Plaintiffs' and Class Members' Private Information is "protected health information" as defined by 45 CFR § 160.103.

97. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

98. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

99. Plaintiffs' and Class Members' Private Information is "unsecured protected health information" as defined by 45 CFR § 164.402.

100. Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

101. Plaintiffs' and Class Members' unsecured PHI acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

102. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and

which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

103. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

104. Even assuming that Defendant's website post is sufficient notice to victims of the Data Breach, which it is not, after receiving such notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

105. The Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of Private Information when it was no longer necessary and/or had honored its obligations to Plaintiffs and Class Members.

106. It can be inferred from Defendant's Data Breach that it either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiffs and Class Members' Private Information.

107. Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

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

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(4);

j. 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

k. 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);

l. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*; and

m. Retaining information past a recognized purpose and not deleting it.

108. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

109. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiffs and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the Private Information of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Plaintiffs and Class Members' Private Information remains at risk of subsequent data breaches.

Defendant Failed to Comply with Industry Standards.

110. As noted above, experts studying cyber security routinely identify entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

111. Several best practices have been identified that a minimum should be implemented by employers in possession of Private Information, like Defendant, including but not limited to: educating all employees; 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. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

112. Other best cybersecurity practices that are standard for employers 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. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

113. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

114. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Plaintiff Jeannette Lavoie-Soria's Experience

115. Plaintiff Lavoie-Soria received medical services at the Defendant's Warwick office in 2023.

116. At or around this time, Plaintiff Lavoie-Soria was required to, and did, provide her Private Information to the Defendant, including PII and Social Security Number, as well as her PHI.

117. As a result of the Data Breach, Plaintiff Lavoie-Soria has spent significant time dealing with the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

118. Plaintiff Lavoie-Soria has taken it upon herself to research the Data Breach. She is on a fixed income and protecting her Social Security number is vital to her well-being.

119. As a result of the Data Breach, she has diligently checked all of her accounts to make sure there is no fraud that she can determine.

120. Upon information and belief, Plaintiff Lavoie-Soria's Private Information was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

121. Plaintiff Lavoie-Soria is very careful about sharing Private Information. Plaintiff has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing her Private Information in a safe and secure location. Moreover, Plaintiff diligently chooses unique usernames and passwords for online accounts.

122. Plaintiff Lavoie-Soria has a credit monitoring product and has increased her diligence in checking that her credit is not impacted. She has also reviewed her personal financial accounts, credit reports, and tax information as mandated by the notice on Defendant's website.

123. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff Lavoie-Soria's Private Information is here as a result of the Data Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.

124. Plaintiff Lavoie-Soria has suffered actual injury in the form of damages to and diminution in the value of Private Information—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving orthopedic care from Defendant, which was compromised in and as a result of the Data Breach.

125. In the aftermath of the Data Breach, Plaintiff Lavoie-Soria has observed significant spam emails, texts and calls, which, upon information and belief, include communications that are the result of the Data Breach.

126. Plaintiff Lavoie-Soria has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, especially due to her significant health issues reflected in her PHI and her reliance on SSDI tethered to her Social Security number.

127. Plaintiff Lavoie-Soria is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from Private Information being placed in the hands of unauthorized third parties and criminals.

128. Plaintiff Lavoie-Soria has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches. She would not have provided her Private Information had she known of the Defendant's lax data security procedures.

Plaintiff Rebecca Reilly's Experience

129. Plaintiff Reilly received medical services at one of Defendant's offices.

130. At or around this time, Plaintiff Reilly was required to, and did, provide her Private Information to the Defendant, including PII and Social Security Number, as well as her PHI.

131. As a result of the Data Breach, Plaintiff Reilly has spent significant time dealing with the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

132. Plaintiff Reilly has taken it upon herself to research the Data Breach.

133. As a result of the Data Breach, she has diligently checked all of her accounts to make sure there is no fraud that she can determine.

134. Upon information and belief, Plaintiff Reilly's Private Information was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

135. Plaintiff Reilly is very careful about sharing Private Information. Plaintiff has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing her Private Information in a safe and secure location. Moreover, Plaintiff diligently chooses unique usernames and passwords for online accounts.

136. Plaintiff Reilly has a credit monitoring product and has increased her diligence in checking that her credit is not impacted. She has also reviewed her personal financial accounts, credit reports, and tax information as mandated by the notice on Defendant's website.

137. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff Reilly's Private Information is here as a result of the Data Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.

138. Plaintiff Reilly has suffered actual injury in the form of damages to and diminution in the value of Private Information—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving orthopedic care from Defendant, which was compromised in and as a result of the Data Breach.

139. Plaintiff Reilly has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, especially due to her significant health issues reflected in her PHI and her reliance on SSDI tethered to her Social Security number.

140. Plaintiff Reilly is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from Private Information being placed in the hands of unauthorized third parties and criminals.

141. Plaintiff Reilly has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches. She would not have provided her Private Information had she known of the Defendant's lax data security procedures.

Plaintiff Frederick Whelan's Experience

142. Plaintiff Whelan received medical services at one of Defendant's offices in or around 2010.

143. At or around this time, Plaintiff Whelan was required to, and did, provide his Private Information to the Defendant, including PII like his full name, address, date of birth, as well as his PHI.

144. Plaintiff received a Notice of Data Breach on or around December 9, 2024.

145. Through its Data Breach, Defendant compromised Plaintiff's full name, address, date of birth, and sensitive medical information.

146. As a result of the Data Breach, Plaintiff Whelan has spent significant time dealing with the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

147. Plaintiff Whelan has taken it upon himself to research the Data Breach.

148. As a result of the Data Breach, he has diligently checked all of his accounts to make sure there is no fraud that he can determine.

149. Upon information and belief, Plaintiff Whelan's Private Information was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

150. Plaintiff Whelan is very careful about sharing his Private Information. Plaintiff has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing his Private Information in a safe and secure location. Moreover, Plaintiff diligently chooses unique usernames and passwords for online accounts.

151. Plaintiff Whelan has increased his diligence in checking that his credit is not impacted. He has also reviewed his personal financial accounts, credit reports, and tax information as mandated by Defendant's breach notice.

152. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff Whelan's Private Information is here as a result of the Data Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.

153. Plaintiff Whelan has suffered actual injury in the form of damages to and diminution in the value of Private Information—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving orthopedic care from Defendant, which was compromised in and as a result of the Data Breach.

154. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam calls, texts and emails, suggesting that his Private Information is already in the hands of cybercriminals as a result of the Data Breach.

155. Plaintiff Whelan has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, especially due to his health issues reflected in his PHI.

156. Plaintiff Whelan is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and criminals.

157. Plaintiff Whelan has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches. He would not have provided his Private Information had he known of the Defendant's lax data security procedures.

Plaintiff Patricia Robinson's Experience

158. Plaintiff Robinson received medical services at one of Defendant's offices in or around 2022.

159. At or around this time, Plaintiff Robinson was required to, and did, provide her Private Information to the Defendant, including PII like her full name, address, date of birth, financial information, as well as his PHI.

160. Plaintiff Robinson received a Notice of Data Breach on or around December 9, 2024.

161. Through its Data Breach, Defendant compromised Plaintiff Robinson's PII/PHI, including her full name, address, date of birth, and sensitive medical information.

162. As a result of the Data Breach, Plaintiff Robinson has spent significant time dealing with the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

163. Plaintiff Robinson has taken it upon herself to research the Data Breach.

164. As a result of the Data Breach, Plaintiff Robinson has and continues to diligently monitor all of her accounts for unauthorized activities and transactions.

165. Upon information and belief, Plaintiff Robinson's Private Information was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

166. Plaintiff Robinson is very careful about sharing her Private Information. Plaintiff has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing her Private Information in a safe and secure location. Moreover, Plaintiff diligently chooses unique usernames and passwords for online accounts.

167. Plaintiff Robinson has increased her diligence in checking that her credit is not impacted. She has also reviewed his personal financial accounts, credit reports, and tax information as mandated by Defendant's Breach Notice.

168. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff Robinson's Private Information is here as a result of the Data Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.

169. Plaintiff Robinson has suffered actual injury in the form of damages to and diminution in the value of Private Information—a form of intangible property that Plaintiff Robinson entrusted to Defendant for the purpose of receiving orthopedic care from Defendant, which was compromised in and as a result of the Data Breach.

170. And in the aftermath of the Data Breach, Plaintiff Robinson has suffered from a spike in spam and scam calls, texts and emails, suggesting that her Private Information is already in the hands of cybercriminals as a result of the Data Breach.

171. Plaintiff Robinson has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, especially due to her health issues reflected in her PII and PHI.

172. Plaintiff Robinson is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and criminals.

173. Plaintiff Robinson has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches. She would not have provided her Private Information had she known of the Defendant's lax data security procedures.

Plaintiff Aria E. DiMeo's Experience

174. Plaintiff Aria E. DiMeo is a patient of Defendant.

175. To receive medical services from Defendant, Plaintiff DiMeo was required to, and did, provide her Private Information to the Defendant, including PII and Social Security Number, as well as her PHI.

176. Plaintiff Aria E. DiMeo received Defendant's data breach notice. The notice informed Plaintiff that her Private Information was improperly accessed and obtained by third parties and that this information could include her name, address, date of birth, billing and claims information, health insurance claims information, and medical information, including diagnosis, medications, test results, x-ray images, and other treatment information.

177. As a result of the Data Breach, Plaintiff DiMeo has spent significant time dealing with the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

178. After Defendant's Data Breach, Plaintiff DiMeo experienced a sizable increase in the number of spam calls and messages. She reasonably believes this increase is a result of the Data Breach.

179. As a result of the Data Breach, Plaintiff DiMeo has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff DiMeo has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

180. As a result of the Data Breach, Plaintiff DiMeo has suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her Private Information for purposes of identity theft and fraud. Plaintiff DiMeo is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

181. Plaintiff DiMeo is very careful about sharing Private Information. Plaintiff has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing her Private Information in a safe and secure location. Moreover, Plaintiff diligently chooses unique usernames and passwords for online accounts.

182. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff DiMeo's Private Information is here as a result of the Data Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.

183. Plaintiff DiMeo suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

184. As a result of the Data Breach, Plaintiff DiMeo anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, she is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Upon information and belief, Plaintiff DiMeo's Private Information remains on Defendant's computer systems unencrypted.

185. Plaintiff DiMeo is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from Private Information being placed in the hands of unauthorized third parties and criminals.

186. Plaintiff DiMeo has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches. She would not have provided her Private Information had she known of the Defendant's lax data security procedures.

V. CLASS ALLEGATIONS

187. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated pursuant to R.I. Super. R. Civ. P. 23 and other applicable law.

188. The Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose Private Information was compromised during the Data Breach that occurred between September 4, 2024 and

September 8, 2024 (the "Class").

189. Excluded from the Class is the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which a Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

190. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

191. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class-wide relief because Plaintiffs and all members of the Class were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

192. The Class is so numerous that individual joinder of its members is impracticable.

193. Common questions of law and fact exist as to members of the Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had a duty not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether 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;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

194. Plaintiffs are members of the Class they seek to represent, and their claims and injuries are typical of the claims and injuries of the other Class Members.

195. Plaintiffs will adequately and fairly protect the interests of other Class Members. Plaintiffs have no interests adverse to the interests of absent Class Members. Plaintiffs are represented by legal counsel with substantial experience in class action litigation. The interests of Class Members will be fairly and adequately protected by Plaintiffs and their counsel.

196. Defendant has acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

197. A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiffs are unaware of any difficulties that are likely to be encountered in the management of

this action that would preclude its maintenance as a class action.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

198. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in the paragraphs above.

199. Plaintiffs and the Class provided and entrusted Defendant with certain Private Information as a condition of receiving orthopedic services based upon the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

200. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

201. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

202. Defendant had a duty to exercise reasonable care in overseeing, safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiffs and the Class in Defendant's possession was adequately secured and protected.

203. Defendant owed a duty to Plaintiffs and the Class to implement intrusion detection processes that would detect a data breach or unauthorized access to its systems in a timely manner.

204. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain pursuant to regulations, including that of former patients.

205. Defendant also had a duty to employ proper procedures to detect and prevent the improper access, misuse, acquisition, and/or dissemination of the Private Information of Plaintiffs and the Class.

206. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between both Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of their relationship with Defendant.

207. Defendant owed a duty to disclose the material fact that Defendant's data security practices were inadequate to safeguard the Private Information of Plaintiffs and the Class.

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

209. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's system.

210. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included

its decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiffs and the Class, including basic encryption techniques freely available to Defendant.

211. Plaintiffs and the Class had no ability to protect their Private Information that was in, and likely remains in, Defendant's possession.

212. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

213. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession, how it was compromised, and precisely the types of data that was compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties. No direct notice has been provided.

214. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully accessed, acquired, and/or released to unauthorized third persons as a result of the Data Breach.

215. Defendant, through their actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiffs and the Class during the time the Private Information was within Defendant's possession or control.

216. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

217. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Plaintiffs and the Class in the face of increased risk of theft.

218. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect unauthorized access or intrusions and prevent dissemination of their Private Information. Additionally, Defendant failed to disclose to Plaintiffs and the Class that Defendant's security practices were inadequate to safeguard the Private Information of Plaintiffs and the Class.

219. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Private Information it was no longer required to retain pursuant to regulations, including Private Information of former patients.

220. Defendant, through their actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

221. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

222. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures and oversight.

223. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer injury.

224. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private

Information which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

225. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

226. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in the paragraphs above.

227. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

228. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

229. Defendant violation of Section 5 of the FTC Act constitutes negligence *per se*.

230. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

231. The harm that occurred because of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, because 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.

232. Defendant's violations of HIPAA and HITECH also independently constitute negligence *per se*.

233. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

234. Plaintiffs and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

235. The harm that occurred because of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

236. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and the Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

237. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in the paragraphs above.

238. Defendant required Plaintiffs and the Class to provide and entrust their Personal Information as a condition of receiving orthopedic services with Defendant.

239. Plaintiffs and the Class paid money to Defendant in exchange for services, as well as Defendant's promises to protect their protected health information and other Private Information from unauthorized disclosure.

240. Defendant promised to comply with HIPAA and HITECH standards and to make sure that Plaintiffs and Class Members' Private Information would remain protected.

241. As a condition of obtaining medical services from Defendant, Plaintiffs and the Class provided and entrusted their Private Information. In so doing, Plaintiffs the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such

information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

242. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete Private Information and to pay Defendant in exchange for Defendant's collective agreement to, *inter alia*, protect their Private Information.

243. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of Defendant's implied promise to adequately safeguard this confidential personal and medical information.

244. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

245. Defendant has breached the implied contracts it made with Plaintiffs and the Class by making their Private Information accessible from the internet (regardless of any mistaken belief that the information was protected) and failing to make reasonable efforts to use the latest security technologies designed to help ensure that the Private Information was secure, failing to encrypt Plaintiffs and Class Members' Private Information, failing to safeguard and protect their Private Information, and by failing to provide timely and accurate notice to them that Private Information was compromised as a result of the data breach.

246. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to comply with its promise to abide by HIPAA and HITECH.

247. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

248. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

249. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

250. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

251. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

252. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

253. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

254. Defendant further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that

is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

255. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing both oversight and physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

256. Defendant further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

257. Defendant's failure to meet these promises constitutes a breach of the implied contracts.

258. Because Defendant allowed unauthorized access to Plaintiffs and Class Members' Private Information and failed to safeguard the Private Information, Defendant breached its contracts with Plaintiffs and Class Members.

259. Defendant breached its contracts by not meeting the minimum level of protection of Plaintiffs and Class Members' protected health information and other Private Information, because Defendant did not prevent against the Data Breach.

260. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing medical services to Plaintiffs and Class Members that were of a diminished value.

261. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class are now subject to the present and continuing risk of fraud, and are suffering (and will continue to suffer) the ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality

of the stolen confidential data; the diminished value of services provided by Defendant; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

262. As a result of Defendant's breach of implied contract, Plaintiffs and the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

263. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in the paragraphs above.

264. This Count is pled in the alternative to Count III, Breach of Implied Contract.

265. Plaintiffs and the Class conferred a benefit upon Defendant in providing Private Information to Defendant.

266. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and the Class. Defendant also benefited from the receipt of Plaintiffs' and the Class's Private Information, as this was used to facilitate its services to Plaintiffs and the Class.

267. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

268. Instead of providing a reasonable level of security, or retention policies, which would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and the Class by utilizing cheaper, ineffective security

measures. Plaintiffs and the Class, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

269. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and the Class's Private Information because Defendant failed to adequately protect it.

270. Plaintiffs and the Class have no adequate remedy at law.

271. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

272. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in the paragraphs above.

273. Given the relationship between Defendant and Plaintiffs and the Class, where Defendant became guardian of Plaintiffs' and Class Members' Private Information, Defendant became fiduciaries by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and the Class, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

274. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their Private Information.

275. Because of the highly sensitive nature of the Private Information, Plaintiffs and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

276. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' Private Information.

277. Defendant also breached its fiduciary duty to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

278. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

279. As a result of Defendant's breach of fiduciary duty, Plaintiffs and the Class are entitled to and demand actual, consequential, and nominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

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

ii. prohibiting Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information

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

iv. requiring Defendant to delete, destroy, and purge the personal identifying information 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;

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

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party

security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, 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 system;

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

xi. 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 personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant 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 Defendant's policies, programs, and systems for protecting personal identifying information;

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

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

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, nominal, and statutory damages, as allowed by law in an amount to be determined;

E. For an award of restitution and damages in an amount to be determined;

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

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: January 27, 2025

Respectfully Submitted,

/s/ Vincent L. Greene
Vincent L. Greene, Esq. (#5971)
MOTLEY RICE LLC
40 Westminster Street, 5th Floor
Providence, RI 02903
Tel: (401)-457-7730
Fax: (401) 457-7708
vgreene@motleyrice.com

Kenneth J. Grunfeld
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
grunfeld@kolawyers.com

Peter N. Wasylyk (RI Bar # 3351)
LAW OFFICES OF PETER N. WASYLYK
1307 Chalkstone Avenue
Providence, Rhode Island 02908
Tel: (401) 831-7730 / Fax: (401) 861-6064
E-mail: pnwlaw@aol.com

Leanna A. Loginov (*pro hac vice forthcoming*)
SHAMIS & GENTILE, P.A.
14 NE 1st Ave, Ste 705
Miami, FL 33132
Tel: (305) 479-2299
lloginov@shamisgentile.com

Danielle L. Perry (*pro hac vice forthcoming*)
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
E-mail: dperry@masonllp.com

Nickolas J. Hagman (*pro hac vice* forthcoming)
CAFFERTY CLOBES
MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
nhagman@caffertyclobes.com

Counsel for Plaintiffs and the Putative Class

CERTIFICATION

I hereby certify that on this 27th day of January, 2025, I caused a true copy of the within document to be filed via the Rhode Island Judiciary's Electronic Filing System where it is available for viewing and or downloading.

Susan E. Hargreaves

ClassAction.org