**UNITED STATES DISTRICT COURT**
**DISTRICT OF COLORADO**

| | |
|---|---|
| DAVE MARCO, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>WESTERN ORTHOPAEDICS, P.C.,<br><br>Defendant. | Case No. 1:26-cv-2074<br><br>**CLASS ACTION**<br><br>**JURY TRIAL DEMANDED** |

## CLASS ACTION COMPLAINT

Plaintiff Dave Marco ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through his attorneys, brings this Class Action Complaint against Defendant Western Orthopaedics, P.C. ("Western Ortho" or "Defendant"), and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

## INTRODUCTION

1. Plaintiff brings this class action against Western Ortho for its failure to secure and safeguard the personally identifying information ("PII") and personal health information ("PHI") of approximately 113,330 of its current and former patients (including Plaintiff's), including names, addresses, phone numbers, Social Security numbers, dates of birth, financial accounts, credit, or debit card numbers, health insurance information, health insurance plan or subscriber identification number, medical provider name, medical dates of service, and medical cost or billing information.

2. Western Ortho is an orthopedic surgery practice that treats various musculoskeletal injuries.

3. Between approximately September 17, 2025 and September 25, 2025, an unauthorized third party gained access to Western Ortho's network systems and obtained files containing the PII/PHI of Western Ortho's current and former patients, including Plaintiff (the "Data Breach").

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

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

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

## PARTIES

***Plaintiff Dave Marco***

7. Plaintiff Dave Marco is a citizen of Colorado.

8. Plaintiff is a former patient of Western Ortho. As a condition of providing services to Plaintiff, Western Ortho required Plaintiff to provide it with his PII/PHI.

9. Plaintiff believed Western Ortho had implemented and maintained reasonable security and practices to protect his PII/PHI. With this belief in mind, Plaintiff provided his PII/PHI to Western Ortho in connection with obtaining services from Western Ortho.

10. At all relevant times Western Ortho stored and maintained Plaintiff's PII/PHI on its network systems, including the systems accessed in the Data Breach.

11. Had Plaintiff known that Western Ortho does not adequately protect the PII/PHI in its possession, he would not have obtained services from Western Ortho or agreed to entrust it with his PII/PHI.

12. Plaintiff received notice from Western Ortho notifying him that his PII/PHI was affected in the Data Breach.

13. After the Data Breach occurred, Plaintiff has experienced an increase in the number of spam calls and emails that he receives.

14. In or about April 2026, Plaintiff began receiving calls from a debt collector trying to get him to pay alleged debts that he did not owe.

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

***Defendant Western Orthopaedics, P.C.***

16. Defendant Western Orthopaedics, P.C. is a Colorado professional corporation with its principal place of business located at 500 E Hampden Ave, Ste 400, Englewood CO 80113.

Western Ortho can be served through its registered agent, Edward Hudson Parks, at 500 E Hampden Ave, Ste 400, Englewood CO 80113.

## JURISDICTION AND VENUE

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

18. This Court has personal jurisdiction over Defendant because it has its principal place of business in Colorado and was formed in Colorado.

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

## FACTUAL ALLEGATIONS

### *Overview of Western Ortho*

20. Western Ortho is an orthopedic surgery practice that traces back its history to 1938.[1] Its physicians "treat and manage the symptoms of a wide variety of musculoskeletal conditions, including sports injuries and spinal conditions."[2]

21. In the regular course of its business, Western Ortho collects and maintains the PII/PHI of its current and former patients. Western Ortho required Plaintiff and Class members to provide it with their PII/PHI as a condition of providing them with healthcare services.

[1] *Our History*, WESTERN ORTHO, https://www.western-ortho.com/contents/about/our-history (last accessed May 13, 2026).
[2] *About*, WESTERN ORTHO, https://www.western-ortho.com/about (last accessed May 13, 2026).

22. Plaintiff and Class members are current or former patients of Western Ortho who entrusted Western Ortho with their PII/PHI.

***The Data Breach***

23. Between approximately September 17, 2025 and September 25, 2025, an unauthorized third party had access to Western Ortho's network systems, which Western Ortho discovered on or about October 2, 2025.[3] After an investigation, Western Ortho determined that files were accessed and acquired in the Data Breach and that the compromised data included PII/PHI, including that of Plaintiff and Class members. The PII/PHI affected in the Data Breach included the following data elements: "full name and address; phone number; Social Security number; date of birth; financial account, credit, or debit card number, with or without any required security code, access code, or password; and protected health information, including health insurance information, health insurance plan or subscriber identification number, medical provider name, medical dates of service, and medical cost or billing information."[4]

24. The PEAR ransomware group "claimed responsibility for the [Data Breach] and proceeded to leak the stolen data when the ransom was not paid."[5] The group "is a newly surfaced actor" that "favors a low-noise, high-pressure approach, gaining access quietly before deploying encryption and extortion tactics."[6] Accordingly, Plaintiff's and Class members' PII/PHI is available on the dark web for the use of cybercriminals.

---

[3] *Notice of Data Breach*, MASS.GOV, https://www.mass.gov/doc/2026-684-western-orthopaedics-pc/download (last accessed May 13, 2026).
[4] *Id.*
[5] Steve Adler, *Data Breaches Announced by Four Healthcare Providers*, THE HIPAA JOURNAL (May 7, 2026), https://www.hipaajournal.com/data-breaches-four-healthcare-providers-may-2026/.
[6] *PEAR*, BLACKFOG, https://www.blackfog.com/cybersecurity-101/pear/ (last accessed May 13, 2026).

25. Western Ortho recognizes the risk of serious harm Plaintiff and Class members now face as a result of the Data Breach. For example, the data breach notice Western Ortho sent to those affected recommends that Plaintiff and Class members monitor their explanation of benefits statements, place a fraud alert on their credit file, initiate a credit freeze, and monitor their credit report, among other practices.[7]

26. Despite learning of the Data Breach on or about October 2, 2025, Western Ortho did not begin notifying Plaintiff and Class members of the Data Breach until in or about May 2026, approximately seven months after it learned of the Data Breach. Western Ortho's failure to promptly notify Plaintiff and Class members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

***Defendant Knew that Criminals Target PII/PHI***

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

28. It is well known among companies that store sensitive personally identifying information that such information—such as the PII/PHI stolen in the Data Breach—is valuable

[7] *Notice of Data Breach*, *supra* n. 3.

and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[8]

29. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2025 report, Kroll found that "the healthcare industry was the most breached" in 2024.[9] The company found that 23% of the breaches that it handled responses for were from the healthcare industry, up from 18% in 2023.[10]

30. PII/PHI is a valuable property right.[11] The value of PII/PHI as a commodity is measurable.[12] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[13] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[14] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

---

[8] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[9] *Data Breach Outlook*, KROLL, https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2025 (last accessed May 13, 2026).

[10] *See id*.

[11] *See* Marc van Lieshout, *The Value of Personal Data*, 457 Int'l Fed'n for Info. Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[12] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[13] Organization for Economic Co-operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[14] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party*

31. Criminals piece together bits and pieces of compromised PII/PHI for profit by creating "Fullz" packages. "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more.

32. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII/PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

33. The development of "Fullz" packages means that the stolen PII/PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and Class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI that was exfiltrated in the Data Breach, criminals may still 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.

34. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to criminals.

35. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data

---

*Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

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

37. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[17] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[18]

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

[15] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").
[16] *Id.*
[17] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.
[18] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[19] Steager, *supra* note 15.

disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[20]

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

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

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

41. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[22] [23]

---

[20] *Id.*

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

[22] *See* Federal Trade Commission, *What to Know About Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed May 13, 2026).

[23] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

42. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[24]

43. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[25]

44. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[26] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[27] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [28] The FTC also warns, "If the thief's health information is mixed with yours it

---

[24] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[25] Identity Theft Resource Center, *2025 Consumer Impact Report*, IDENTITY THEFT RES. CTR. (2025), https://www.idtheftcenter.org/publication/itrc-2025-consumer-impact-report/ (last accessed May 13, 2026).

[26] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIV. F. (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[27] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 18.

[28] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed May 13, 2026).

could affect the medical care you're able to get or the health insurance benefits you're able to use."[29]

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

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services neither sought nor received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own. [30]

46. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately

[29] *Id*.
[30] *See* Dixon & Emerson, *supra* note 26.

three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[31]

47. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was specifically targeted and taken by someone intending to use that information for any number of improper purposes, fraud, and scams, including making the information available for sale on the black-market.

***Damages Sustained by Plaintiff and Class Members***

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

## CLASS ALLEGATIONS

49. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

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

[31] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

> All persons whose personally identifiable information and personal health information was accessed and disclosed in the Data Breach to unauthorized persons, including all who were sent a notice of the Data Breach.

51. Excluded from the Class are Western Orthopaedics, P.C., and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge.

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

53. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. Western Ortho reported to the United States Department of Health and Human Services that the Data Breach affected 113,330 persons.[32]

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

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

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

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

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

[32] *HIPAA Cases Currently Under Investigation*, U.S. Dept. of Health and Human Services, Office of Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf (last accessed May 13, 2026).

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

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

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

56. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

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

58. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress from Defendant's wrongful conduct. Even if Class members

could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

## CAUSES OF ACTION

### COUNT I
### NEGLIGENCE

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

60. Western Ortho owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in its possession, custody, or control.

61. Western Ortho knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Western Ortho knew or should have known of the many data breaches that targeted healthcare providers that collect and store PII/PHI in recent years.

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

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

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

65. But for Western Ortho's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

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

## COUNT II
## NEGLIGENCE PER SE

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

68. Defendant's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

69. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to employ reasonable measures to protect and secure PII/PHI.

70. Defendant violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

71. Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitute negligence per se.

72. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

73. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

74. It was, or should have been, reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members'

PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

75. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Western Ortho's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

## COUNT III
## BREACH OF FIDUCIARY DUTY

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

77. Plaintiff and Class members gave Western Ortho their PII/PHI in confidence, believing that Western Ortho would protect that information. Plaintiff and Class members would not have provided Western Ortho with this information had they known it would not be adequately protected. Western Ortho's acceptance and storage of Plaintiff's and Class

members' PII/PHI created a fiduciary relationship between Western Ortho and Plaintiff and Class members. In light of this relationship, Western Ortho must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class members' PII/PHI.

78. Due to the nature of the relationship between Western Ortho and Plaintiff and Class members, Plaintiff and Class members were entirely reliant upon Western Ortho to ensure that their PII/PHI was adequately protected. Plaintiff and Class members had no way of verifying or influencing the nature and extent of Western Ortho's data security policies and practices, and Western Ortho was in an exclusive position to guard against the Data Breach.

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

80. As a direct and proximate result of Western Ortho's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Western Ortho's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of

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

**COUNT IV**
**BREACH OF IMPLIED CONTRACT**

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

82. In connection with receiving healthcare services, Plaintiff and all other Class members entered into implied contracts with Western Ortho.

83. Pursuant to these implied contracts, Plaintiff and Class members paid money to Western Ortho, directly or through their insurance, and provided Western Ortho with their PII/PHI. In exchange, Western Ortho agreed to, among other things, and Plaintiff and Class members understood that Western Ortho would: (1) provide healthcare services to Plaintiff and Class members; (2) collect, maintain, and utilize Plaintiff's and Class members' PII/PHI to, among other things, facilitate treatment and the provision of healthcare services to Plaintiff and Class members; (3) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; (4) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations, industry standards, and Western Ortho's representations; and (5) maintain the confidentiality of Plaintiff's and Class members' PII/PHI and protect it from unauthorized access, disclosure, theft, and misuse.

84. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Western Ortho, on the other hand. Had Plaintiff and Class members known that Western Ortho would not adequately protect its patients' PII/PHI, they would not have agreed to provide Western Ortho with their PII/PHI or received healthcare services from Western Ortho.

85. Plaintiff and Class members performed their obligations under the implied contract when they provided Western Ortho with their PII/PHI and paid—directly or through their insurers—for healthcare services from Western Ortho.

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

87. Western Ortho's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

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

## COUNT V
## UNJUST ENRICHMENT

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

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

91. Plaintiff and Class members conferred a monetary benefit upon Western Ortho in the form of monies paid for healthcare services and through the provision of their PII/PHI.

92. Western Ortho accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Western Ortho also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate its healthcare operations and billing services.

93. As a result of Western Ortho's conduct, Western Ortho's current and former patients suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that patients paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

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

95. Plaintiff and Class members have no adequate remedy at law.

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

## PRAYER FOR RELIEF

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

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

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

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

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

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

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

## JURY TRIAL DEMANDED

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

Dated: May 13, 2026

Respectfully submitted,

/s/ Ben Barnow

Ben Barnow
Anthony L. Parkhill
**BARNOW AND ASSOCIATES, P.C.**
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

*Counsel for Plaintiff*