IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

CRAIG MEJIA, individually and on behalf of all others similarly situated, Plaintiff, v. WRIGHT & FILIPPIS, INC., Defendant.	Case No: 22-12914 **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Craig Mejia ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint and alleges the following against Defendant Wright & Filippis, Inc. ("Wright & Filippis" or "Defendant"), based upon personal knowledge with respect to Plaintiff and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach (the "Data Breach") involving Wright & Filippis, which collected and stored certain private health information ("PHI") of the Plaintiff and the putative Class Members, all of whom have PHI on Wright & Filippis servers.

2. According to Wright & Filippis, the PHI compromised in the Data Breach "may have" included highly-sensitive information including but not limited to name, date of birth, patient number, Social Security numbers, financial account numbers, and health insurance information.

3. Social Security numbers are particularly valuable to criminals. This information can be sold and traded on black markets within the dark web. The loss of a Social Security number is particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

4. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PHI. Inexplicably, the Defendant has acknowledged that the cybersecurity attack occurred in *January* of 2022, but it has only recently begun contacting Class Members.

5. According to the U.S. Department of Health and Human Services, the Data Breach has affected 877,584 individuals.[1]

[1] *Cases Currently Under Investigation*, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Dec. 1, 2022) (attached hereto at Exhibit A).

6. Plaintiff brings this class action lawsuit on behalf of himself and all those similarly situated to address Defendant's inadequate safeguarding of Class Members' PHI that it had collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was unsecured and left open to the unauthorized access of any unknown third party.

PARTIES

7. Plaintiff Craig Mejia is an adult individual and citizen of the State of Michigan who resides in Manistee, Michigan.

8. Plaintiff is a former client of Defendant; Plaintiff had entered into a transaction with Defendant in order to have Defendant perform foot molding work.

9. On November 18, 2022, Plaintiff was notified by Wright & Filippis via letter of the Data Breach and of the impact to his PHI.

10. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time and expenses related to monitoring his financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of his personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

11. Defendant Wright & Filippis is a manufacturing company with its principal place of business and headquarters at 2845 Crooks Rd, Rochester Hills, Michigan 48309.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this controversy pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class Members who are citizens of states other than Defendant's state of citizenship.

13. This Court has personal jurisdiction over Defendant because it is authorized to and does conduct substantial business in this District, and is a citizen of this District by virtue of its headquarters and principal place of business being located in this District.

14. Venue is proper under 28 U.S.C. §1391(b) because the cause of action upon which the complaint is based arose in Rochester Hills, Michigan, which is in the Eastern District of Michigan.

COMMON FACTUAL ALLEGATIONS

15. Plaintiff and the proposed Class are, or were, patients and/or consumers of Wright & Filippis. Wright & Filippis specializes in the design and manufacture of prosthetics, orthotics, and accessibility solutions.

16. As noted above, Plaintiff brings this class action against Defendant for Defendant's failure to properly secure and safeguard protected health information as defined by the Health Insurance Information Portability and Accountability Act ("HIPAA"), medical information, and other personally identifiable information, for failing to comply with industry standards to protect and safeguard that information, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other members of the Class that such information had been compromised.

Wright & Filippis' Unsecure Data Management and Disclosure of Data Breach

17. Plaintiff and Class Members provided their PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

18. Plaintiff and Class Member's PHI was provided to Defendant in conjunction with the type of work Defendant does within the healthcare industry, specifically the provision of prosthetics and orthotics to their patients and consumers.[2]

[2] Kayla Clark, *Current, former patients of Wright and Filippis may have been impacted by data breach*, Click On Detroit (Nov. 29, 2022), https://www.clickondetroit.com/news/local/2022/11/29/current-former-patients-of-wright-and-filippis-may-have-been-impacted-by-data-breach/ (last visited Nov. 30, 2022) (attached hereto at Exhibit B).

19. However, Defendant Wright & Filippis failed to secure the PHI of the individuals that provided Defendant with this sensitive information.

20. Wright & Filippis' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date Defendant disclosed the incident.

21. Indeed, Wright & Filippis notes that it is "committed to ensuring that your information is secure" on its website.[3]

22. According to Wright & Filippis, the incident stemmed from a "cybersecurity attack cumulating in ransomware from January 26 to January 28, 2022."[4] Wright & Filippis said that "its security detected and terminated the ransomware" shortly thereafter.[5] Moreover, it was not until four months later, in May of 2022, that Wright & Filippis even discovered that the Breach may have impacted consumers' PHI.[6]

23. Despite being aware of the breach in January of 2022 – and despite knowing that it involved consumers' PHI in May of 2022 – Wright & Filippis failed

---

[3] *Privacy Policy*, Wright & Filippis, https://www.firsttoserve.com/privacy-policy/ (last accessed Nov. 30, 2022) (attached hereto at Exhibit C).
[4] Brendan Vrabel, *Michigan-based company Wright & Filippis announces past data breach*, (Nov. 28, 2022), https://www.wilx.com/2022/11/28/michigan-based-company-wright-filippis-announces-past-data-breach/ (last accessed Nov. 30, 2022) (attached hereto at Exhibit D).
[5] *Id.*
[6] *Id.*

to take any action to notify Plaintiff or other class members of this breach until at least November 2022.

24. Despite Defendant's acknowledgement that it would "secure" its patients PHI, it failed to take appropriate or even the most basic steps to protect the PHI of Plaintiffs and other class members from being disclosed.

Plaintiff and the Class Have Suffered Injury as a Result of Wright & Filippis' Data Mismanagement

25. As a result of Defendant's failure to implement and follow even the most basic security procedures, Plaintiff's and Class Members' PHI has been and is now in the hands of unauthorized individuals, which may include data thieves, other unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiff and other Class Members now face an increased risk of identity theft, particularly due to the dissemination of their Social Security numbers, and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to Defendant's Data Breach.

26. Plaintiff and other Class Members have had their most personal and sensitive information—their PHI—disseminated to the public at large and have experienced and will continue to experience emotional pain, mental anguish, anxiety, and embarrassment.

27. Plaintiff and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those

impacted are under heightened and prolonged anxiety, as they will be at a heightened risk of being victims of various cybercrimes for years to come.

28. Cyber criminals seek out PHI at a greater rate than other sources of personal information, and the healthcare sector is particularly vulnerable. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July, and the percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[7]

29. Further, a 2022 report released by IBM Security states that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach, and, as of 2022, healthcare data breach costs have hit a new record high.[8]

30. PII/PHI is a valuable property right.[9] "Firms are now able to attain

---

[7] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited Nov. 30, 2022) (attached hereto at Exhibit E).

[8] *Cost of a Data Breach Report 2022*, IBM Security, https://www.ibm.com/downloads/cas/3R8N1DZJ (last visited Nov. 30, 2022) (attached hereto at Exhibit F).

[9] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts

significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[10] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[11] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black market," or the "dark web," for many years.

31. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and, thus, become more valuable to thieves and more damaging to victims.

---

and preferences as possible") (last visited Dec. 1, 2022) (attached hereto at Exhibit G).

[10] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited December 1, 2022) (attached hereto at Exhibit H).

[11] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited Dec. 1, 2022) (attached hereto at Exhibit I).

32. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[12] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[13] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[14]

33. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[15] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can be sold for up to $1,200 to $1,300 each on the black market.[16]

---

[12] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 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.") (last visited Nov. 30, 2022) (attached hereto at Exhibit J).

[13] *Id.*

[14] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 AM), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last visited Nov. 30, 2022) (attached hereto at Exhibit K).

[15] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Nov. 30, 2022) (attached hereto at Exhibit L).

[16] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013),

Criminals can also purchase access to entire-company data breaches from $900 to $4,500.[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]

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

35. Given these facts, any company that transacts business with a consumer, and then compromises the privacy of consumers' PII/PHI, has thus

---

https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market (last visited Nov. 30, 2022) (attached hereto at Exhibit M).

[17] *In the Dark*, VPNOverview.com, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on Nov. 30, 2022) (attached hereto at Exhibit N).

[18] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf. (last visited December 1, 2022) (attached hereto at Exhibit O).

[19] *See* n.8, *supra*.

[20] *Id.*

deprived that consumer of the full monetary value of the consumer's transaction with the company.

36. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("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 PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[21]

37. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[22]

---

[21] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited Nov. 30, 2022) (attached hereto at Exhibit P).

[22] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Nov. 30, 2022) (attached hereto at Exhibit Q).

38. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[23]

39. Wright & Filippis was on notice that the FBI has recently 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)."[24]

40. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their 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

[23] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack,* SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Nov. 30, 2022) (attached hereto at Exhibit R).

[24] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Nov. 30, 2022) (attached hereto at Exhibit S).

> of patients' health and financial information, but also patient access to care.[25]

41. As implied by the above AMA quote, stolen PHI can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and Class Members.

42. Plaintiff and members of the Class, as a whole, must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

43. Once PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Wright & Filippis'

[25] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Nov. 30, 2022) (attached hereto at Exhibit T).

conduct. Further, the value of Plaintiff's and Class Members' PHI has been diminished by its exposure in the Data Breach.

44. As a result of Wright & Filippis' failures, Plaintiff and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their PHI.

45. Plaintiff and the Class suffered actual injury from having PHI compromised as a result of Wright & Filippis' negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PHI, a form of property that Defendant obtained from Plaintiff; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

46. For the reasons mentioned above, Wright & Filippis' conduct, which allowed the Data Breach to occur, caused Plaintiff, and members of the Class, the significant injuries and harm described above.

47. Plaintiff brings this class action against Defendant for Defendant's failure to properly secure and safeguard PHI and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PHI had been compromised.

48. Plaintiff, individually and on behalf of all other similarly situated individuals, alleges claims in negligence, negligence per se, breach of implied

contract, breach of fiduciary duty, unjust enrichment, and violation of the Michigan Consumer Protection Act.

CLASS ACTION ALLEGATIONS

49. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

50. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons in the United States whose PHI was compromised in the Data Breach as disclosed by Wright & Filippis in or around November 18, 2022 (the "Nationwide Class").

51. Plaintiff proposes the following Subclass definition, subject to amendment as appropriate:

> All persons in the State of Michigan whose PHI was compromised in the Data Breach as disclosed by Wright & Filippis on November 18, 2022 (the "Michigan Subclass").

52. Excluded from the Classes are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

53. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Classes meet the criteria for certification under Rule 23(a), 23(b)(2), 23(b)(3), and 23(c)(4).

54. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. As noted above, there are reportedly 877,584 Class Members.

55. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common question of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PHI;

b. 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;

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

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

e. Whether Defendant owed a duty to Class Members to safeguard their

PHI;

f. Whether Defendant breached its duty to Class Members to safeguard their PHI;

g. Whether computer hackers obtained Class Members' PHI in the Data Breach;

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

i. Whether Defendant's conduct was negligent;

j. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

k. Whether Defendant's acts breaching an implied contract that it had formed with Plaintiff and the Class Members;

l. Whether Defendant violated the Federal Trade Commission Act ("FTC Act");

m. Whether Defendant violated the Health Insurance Portability and Accountability Act ("HIPAA");

n. Whether Defendant was unjustly enriched to the detriment of Plaintiff and the Class;

o. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

p. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

56. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PHI, like that of every other Class Member, was compromised in the Data Breach.

57. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

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

59. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the

cost of litigating their individual claims would be prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the Parties' resources, and protects the rights of each Class Member.

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

61. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the Parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and safeguarding their PHI;

b. Whether Defendant's data security practices were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PHI; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

62. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

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

72. Wright & Filippis owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PHI in its possession, custody, or control.

73. Wright & Filippis knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class members' PHI and the importance of

maintaining secure systems. Wright & Filippis knew, or should have known, of the many data breaches that targeted healthcare providers in recent years.

74. Given the nature of Wright & Filippis' business, the sensitivity and value of the PHI it maintains, and the resources at its disposal, Wright & Filippis should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

75. Wright & Filippis breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' 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 PHI entrusted to it—including Plaintiff's and Class Members' PHI.

76. It was reasonably foreseeable to Wright & Filippis that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' 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' PHI to unauthorized individuals.

77. But for Wright & Filippis' negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their PHI would not have been compromised.

78. As a result of Wright & Filippis' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other 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 substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PHI; (iii) breach of the confidentiality of their PHI; (iv) deprivation of the value of their PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE

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

80. Wright & Filippis' 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").

81. Wright & Filippis' 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 a business, such as Wright & Filippis, of failing to employ reasonable measures to protect and secure PHI.

82. Wright & Filippis' duties further arise from the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1302(d), *et seq.*

83. Wright & Filippis is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

84. Wright & Filippis 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' PHI and not complying with applicable industry standards. Wright & Filippis' conduct was particularly unreasonable given the nature and amount of PHI it obtains and stores, and the foreseeable consequences of a data breach involving PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

85. Wright & Filippis' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

86. 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.

87. 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.

88. It was reasonably foreseeable to Wright & Filippis that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' 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' PHI to unauthorized individuals.

89. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Wright & Filippis' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs 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 substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial

services for which they are entitled to compensation; (ii) improper disclosure of their PHI; (iii) breach of the confidentiality of their PHI; (iv) deprivation of the value of their PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY

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

91. Plaintiff and Class Members either directly or indirectly gave Wright & Filippis their PHI in confidence, believing that Wright & Filippis – a provider of prosthetics and orthotics – would protect that information. Plaintiff and Class Members would not have provided Wright & Filippis with this information had they known it would not be adequately protected. Wright & Filippis' acceptance and storage of Plaintiff's and Class members' PHI created a fiduciary relationship between Wright & Filippis and Plaintiffs and Class Members. In light of this relationship, Wright & Filippis must act primarily for the benefit of its patients and health plan participants, which includes safeguarding and protecting Plaintiff's and Class Members' PHI.

92. Wright & Filippis 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' PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard the PHI of Plaintiffs and Class Members it collected.

93. As a direct and proximate result of Wright & Filippis' breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will 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 PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their 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 PHI which remains in Wright & Filippis' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PHI compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT

94. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein. This claim is pled in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d).

95. Plaintiff and Class Members conferred a monetary benefit upon Wright & Filippis in the form of monies paid for healthcare services or other services.

96. Wright & Filippis accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Wright & Filippis also benefitted from the receipt of Plaintiff's and Class Members' PHI.

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

98. Wright & Filippis should not be permitted to retain the money belonging to Plaintiffs and Class Members because Wright & Filippis 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.

99. Wright & Filippis 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.

COUNT V
BREACH OF IMPLIED CONTRACT

100. Plaintiff incorporates by reference all preceding factual allegations as though fully set forth herein.

101. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their PHI in order for Wright & Filippis to provide services. In exchange, Defendant entered into implied contracts with Plaintiffs and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PHI and to timely notify them in the event of a data breach.

102. Plaintiff and Class Members would not have provided their PHI to Defendant had they known that Defendant would not safeguard their PHI, as promised, or provide timely notice of a data breach.

103. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

104. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PHI and by failing to provide them with timely and accurate notice of the Data Breach.

105. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members.

COUNT VI
VIOLATION OF THE MICHIGAN CONSUMER PROTECTION ACT
(Mich. Comp. Laws Ann § 445.901, *et. seq.*)

106. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

107. Plaintiff brings this cause of action individually and on behalf of the members of the Michigan Subclass.

108. The Michigan Consumer Protection Act was created to protect Michigan consumers from unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce.

109. Plaintiff and Class Members provided PHI to Defendant pursuant to transactions they engaged in with Defendant as patients and consumers.

110. Defendant has its principal place of business and headquarters in Michigan and transacts with Michigan consumers.

111. Wright & Filippis engaged in deceptive trade practices in the conduct of its business, in violation of Mich. Comp. Laws Ann § 445.901, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

112. Wright & Filippis' deceptive trade practices include:

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

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

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

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

f. Failing to timely and adequately notify Plaintiff, and Michigan Subclass Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Michigan Subclass Members' PHI; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

113. Wright & Filippis' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Wright & Filippis' data security and ability to protect the confidentiality of consumers' PHI.

114. Wright & Filippis' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Michigan Subclass Members, that their PHI was not exposed, and misled Plaintiff and the Michigan Subclass Members into believing they did not need to take actions to secure their identities.

115. Wright & Filippis intended to mislead Plaintiff and Michigan Subclass Members and induce them to rely on its misrepresentations and omissions.

116. Had Wright & Filippis disclosed to Plaintiff and Michigan Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Wright

& Filippis would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Wright & Filippis was trusted with sensitive and valuable PHI regarding, upon information and belief, millions of consumers, including Plaintiff, and the Michigan Subclass. Wright & Filippis accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Wright & Filippis held itself out as maintaining a secure platform for PHI data, Plaintiff and the Michigan Subclass Members acted reasonably in relying on Wright & Filippis' misrepresentations and omissions, the truth of which they could not have discovered.

117. As a direct and proximate result of Wright & Filippis' deceptive trade practices, Plaintiff and Michigan Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PHI.

118. Michigan Subclass Members are likely to be damaged by Wright & Filippis' ongoing deceptive trade practices.

119. Plaintiff and the Michigan Subclass Members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

120. Accordingly, pursuant to Mich. Comp. Law Ann. § 445.901, *et seq.*, Michigan Plaintiffs and Michigan Subclass Members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Those damages are: (a) damage to and diminution in the value of their PHI, a form of property that Defendant obtained from Plaintiff and Michigan Subclass Members; (b) violation of Plaintiff's and Michigan Subclass Members' privacy rights; (c) present and increased risk arising from the identity theft and fraud; and (d) other miscellaneous incidental and consequential damages. In addition, given the nature of Wright & Filippis' conduct, Michigan Plaintiffs and Michigan Subclass Members are entitled to all available statutory, exemplary, treble, and/or punitive damages and attorneys' fees based on the amount of time reasonably expended and equitable relief necessary or proper to protect them from Wright & Filippis' unlawful conduct.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Classes, pray for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class and Subclass;

b. For equitable relief enjoining Wright & Filippis from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PHI;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PHI compromised during the Data Breach;

d. For an order requiring Defendant to pay for not less than seven years of credit monitoring services for Plaintiff and the Class(es);

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h. Pre and post-judgment interest on any amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: December 1, 2022

Respectfully Submitted By:

THE MILLER LAW FIRM, P.C.

/s/ E. Powell Miller

E. Powell Miller (P39487)
Sharon S. Almonrode (P33938)
950 W. University Dr., Suite 300
Rochester, MI 48307
T: (248) 841-2200
F: (248) 652-2852
epm@millerlawpc.com
ssa@millerlawpc.com

SHUB LAW FIRM LLC

Jonathan Shub*
Benjamin F. Johns*
134 Kings Hwy E., Fl. 2,
Haddonfield, NJ 08033
T: (856) 772-7200
F: (856) 210-9088
jshub@shublawyers.com
bjohns@shublawyers.com

Attorneys for Plaintiff and the Proposed Class

**Pro Hac Vice Forthcoming*

ClassAction.org