STATE OF NORTH CAROLINA
COUNTY OF DURHAM

FILED
2022 SEP 12 PM 3:39
DURHAM CO., C.S.C.
BY CMH

IN THE GENERAL COURT OF JUSTICE
SUPERIOR COURT DIVISION
FILE NO: 22 CVS 3533

Daniel Green, as an individual and on behalf of all others similarly situated,

Plaintiff,

v.

EmergeOrtho, P.A.,

Defendant.

COMPLAINT

Class Action

Jury Trial Demanded

Plaintiff Daniel Green ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant EmergeOrtho, P.A. ("EmergeOrtho" or "Defendant"), a North Carolina professional association, to obtain damages, restitution, and injunctive relief from Defendant on behalf of a class of similarly situated individuals, as defined below. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of the recent targeted data breach of the computer network of EmergeOrtho, a North Carolina orthopedic medical practice, whereby an unauthorized third-party accessed Defendant's unsecured (or inadequately secured) computer network and exfiltrated a wealth of unencrypted data (the "Data Breach"), including the removal of the highly sensitive personal information and medical records of approximately 68,661 individuals, including current and former patients (the "Class" or "Class Members").

2. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of loss of the value of their private and confidential information, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

3. Plaintiff brings this suit on his own behalf and for similarly situated individuals whose sensitive personal information was entrusted to Defendant's officials and agents, then compromised, unlawfully accessed, and stolen during the Data Breach. Information compromised in the Data Breach includes individuals' full name, Social Security number, date of birth, financial account information, and other personally identifiable information ("PII"), as well as medical and treatment information, considered protected health information as defined by the HIPAA ("PHI"), all of which Defendant collected and retained on its network (collectively the "Private Information").

4. Plaintiff brings this class action lawsuit on behalf of himself and those similarly situated to address: 1) Defendant's inadequate safeguarding of Class Members' Private Information, 2) Defendant's failure to provide timely and adequate notice to Plaintiff and other Class Members that their Private Information was subject of this Data Breach, and 3) Defendant's failure to notify Plaintiff and Class Members precisely what specific Private Information was accessed and exfiltrated.

5. Defendant maintained Plaintiff's and Class Members' Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition that left it vulnerable to cyberattacks and the exfiltration of Plaintiff's and Class Members' Private Information, as actually happened in this Data Breach.

6. Upon information and belief, a data breach and the potential for improper disclosure

of Private Information entrusted to EmergeOrtho was a known and foreseeable risk, and thus EmergeOrtho was on notice that if it failed to take steps necessary to this Private Information (as it did), highly sensitive PII and PHI would be a dangerous condition and at risk of being stolen.

7. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed patients' Private Information to enable detection of external threats and the prompt discovery of any attempt at intrusion. If EmergeOrtho had done so, it could have reduced or eliminated the injuries and damage suffered by Plaintiff and Class Members.

8. Because of the Data Breach, Plaintiff's and Class Members' Private Information was accessed and exfiltrated by cybercriminals, and upon information and belief, Defendant's systems were not fully operable during its investigation of the Data Breach, resulting in a disruption of its access to Plaintiff's and Class Members' medical records, risking impediments to certain patients' healthcare.

9. In addition, Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves and potentially has been sold or will be sold imminently on the dark web.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false

information to police during an arrest.

11. As a further result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened, imminent, and substantial risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff and Class Members have and may incur out of pocket costs in the future when they pay for, among other things, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. In addition, as a direct and proximate result of the Data Breach and subsequent exfiltration of their Personal Information, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges (as recommended by Defendant), putting alerts on their credit files, and dealing with spam messages and e-mails received as a result of the Data Breach.

14. Plaintiff and Class Members have likewise suffered and will continue to suffer an invasion of their property interest in their own Private Information such that they are entitled to damages for unauthorized access to, theft of, and misuse of their Private Information from Defendant.

15. Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their Private Information, as thieves are likely to use it to obtain money and credit in Plaintiff's and Class Members' names for years.

16. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and/or removed

from the network during EmergeOrtho's Data Breach.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

18. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct asserting claims for negligence, invasion of privacy, breach of implied contract, breach of fiduciary duty, and unjust enrichment.

PARTIES

19. Plaintiff Daniel Green is, and at all times mentioned herein was, an individual citizen of the State of North Carolina, residing in Southport (Brunswick County). Plaintiff Green is and was a patient of EmergeOrtho, who received a Notice of Data Breach Letter indicating that his Private Information was accessed in EmergeOrtho's Data Breach. See attached as Exhibit A.

20. Defendant EmergeOrtho, P.A. is a North Carolina professional association that lists its mailing address as 120 William Penn Plaza, Durham, North Carolina 27704. It states on its website that it has 45 outpatient facilities in 21 North Carolina counties.[1] EmergeOrtho can be served through its registered agent, Corporation Service Company at: 2626 Glenwood Ave., Suite 550, Raleigh, North Carolina 27608.

JURISDICTION AND VENUE

21. Pursuant to N.C. Gen. Stat. § 1-75.4, jurisdiction is proper over the Defendant as it is a registered professional associate in the State of North Carolina, it conducts all or nearly all of its business activities here, it maintains its registered executive office here, and the acts and

[1] https://emergeortho.com/about-us/ (last accessed September 8, 2022).

omissions alleged in this Complaint occurred here.

22. Pursuant to N.C. Gen. Stat. §§ 1-77(2) and 1-82, venue is proper in this Court as Defendant regularly conducts business in this County and because all or nearly all of the wrongful acts giving rise to this Complaint occurred here.

23. This Court has jurisdiction to hear this matter as it is a civil case involving damages that exceed $25,000.

FACTUAL ALLEGATIONS

Defendant's Business

24. Defendant EmergeOrtho is a medical care provider of orthopedic care, offering expertise in conditions of the bones, muscles, and joints. EmergeOrtho services include orthopedic urgent care, diagnostic imaging, physical and occupational therapy, as well as other medical care needs.[2] These services include: Our services include specialty areas of Elbow, Foot & Ankle, Hand & Wrist, Hip, Joint Replacement, Knee, Sports Medicine, Shoulder, Spine, Workers' Compensation, Specialized Injections (ESI), Diagnostic Imaging including X-ray & MRI, as well as Physical & Hand Therapy Services.[3]

25. Defendant serves patients in its 45 outpatient offices, located in 21 plus counties in the North Carolina, from the mountains to the coast. It is largest physician-owned orthopedic practice in the state, including locations that offer treatment 7 days a week.[4]

26. EmergeOrtho's practice locations include several in the Triangle Region as well as in Durham, where it lists its primary mailing address on the North Carolina Secretary of State's website.

---

[2] https://emergeortho.com/ (last accessed September 9, 2022).
[3] https://emergeortho.com/triad-region/ (last accessed September 9, 2022).
[4] https://emergeortho.com/about-us/ (last accessed September 8, 2022).

27. According to EmergeOrtho's website, its various facilities are "linked by one Electronic Health Records system. This enables [its] patients to see an orthopedic specialist at various EmergeOrtho locations, without having to transfer their medical records from one location to the next. If while on vacation in another part of the state, for example, records can be accessed and communicated to [a patient's] primary EmergeOrtho physician."[5]

28. EmergeOrtho heralds that "Our Core Values Define Us," under which it promises its patients "Integrity," including that it:

- Upholds the highest standard of patient privacy and safety;
- Inspires trust and gains respect;
- Maintains a high professional standard of conduct.[6]

29. As it conducts its business, Defendant EmergeOrtho requests, collects, and stores highly sensitive patient information, including Private Information requested from Plaintiff and Class Members (who did provide it to EmergeOrtho) including:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Information relating to individual medical history;
- Insurance information and coverage;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification;

[5] https://emergeortho.com/about-us/ (last accessed September 9, 2022).
[6] *Id.*

- Employer information, and;
- Other information that may be deemed necessary to provide care.

30. Defendant EmergeOrtho may also receive private and personal information from other individuals or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patient's health plan(s), close friends, or family members.

31. In its Notice of Privacy Policies, Defendant pledges that it is "committed to protecting medical information" about its patients. And it acknowledges that it is required by law to: make sure that medical information that identifies a particular patient is kept private; provide patients with a notice of its legal duties and privacy practices as well as their legal rights, with respect to medical information.[7]

32. Thus, Defendant is and was well aware of its legal duties to protect the Private Information of Plaintiff and Class Members, although it failed to do so.

33. On information and belief, EmergeOrtho inadequately trains its employees on cybersecurity policies, fails to enforce those policies, or maintains unreasonable or inadequate security practices and systems.

The Data Breach

34. According to its publicly posted "Notice of Data Privacy Incident"[8] by EmergeOrtho, on May 18, 2022, it "detected and stopped a sophisticated ransomware attack."[9] By August 19, 2022—three months later—EmergeOrtho had "determined that certain patients' information may have been exposed to the unauthorized party, including the following categories

[7] https://emergeortho.com/notice-of-privacy-practices/ (last accessed September 9, 2022).
[8] https://emergeortho.com/ (last accessed September 9, 2022).
[9] *Id.*

of information: first and last name, address, and, in some instances, medical and treatment information, financial account information, date of birth and Social Security number."[10]

35. During those three months after the ransomware attack, however, Plaintiff and Class Members had no idea that their Private Information was breached.

36. Upon information and belief, the cyberattack targeted Defendant due to Defendant's status as a healthcare entity that collects, creates, and maintains PII and PHI. This cyberattack was expressly designed to gain access to private and confidential data, including (among other things) Private Information of current and former patients like Plaintiff and Class Members.

37. EmergeOrtho stated that "detected and stopped a sophisticated ransomware attack," and claims it "moved quickly to initiate a response, which included retaining a leading forensic investigation firm who assisted in conducting an investigation along with the assistance of leading IT specialists to confirm the security of [its] network environment."[11]

38. Clearly EmergeOrtho recognizes that time is of the essence to mitigate the damages of breached data, however, its delayed notification to Plaintiff and Class meant that they were unable to mitigate their own injuries.

39. The Notice Letters that EmergeOrtho sent to its patients, including the Plaintiff and Class Members, are dated August 25, 2022, just over 3 months after the EmergeOrtho knew of the Data Breach. *See* Plaintiff's Notice Letter, attached as Exhibit A.[12]

40. Despite its lag in notification of the Data Breach that affected patients, EmergeOrtho now offers victims of its Data Breach just 12 months of "Single Bureau Credit

---

[10] *Id.*
[11] *Id.*
[12] *See* Notice Letter, Exh. A.

Monitoring/Single Bureau Credit Report/ Single Bureau Credit Score services" so long as the person is over 18 years old.[13]

41. As a consequence of the Data Breach on Defendant's computer systems, highly sensitive Private Information belonging to Plaintiff and Class Members that was supposed to be protected by Defendant was removed from Defendant's network, yet it was not.

42. Based on the Notice of Data Breach Letters he received, which informed Plaintiff that his Private Information was removed from Defendant's network and computer systems, Plaintiff reasonably believes his Private Information was stolen from the Defendant's network (and subsequently sold) in the Data Breach.

43. Further, the removal of the Private Information from Defendant's system – information that included full names, dates of birth, and Social Security numbers (which are the keys to identity theft and fraud) demonstrates that this cyberattack was targeted for the purposes of selling Private Information and committing identity theft.

Healthcare Organizations are Targeted by Cybercriminals

44. Cyberattacks against hospitals and healthcare organizations such as Defendant are targeted. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across US healthcare organizations. Significant security incidents are a near-universal experience in US healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets."[14] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable

---

[13] *Id.*

[14] *HIMMS Healthcare Cybersecurity Survey*, HIMSS, https://www.himss.org/himss-cybersecurity-survey (last accessed September 8, 2022).

information (PII) for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[15]

45. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

46. Plaintiff and Class Members provided their Private Information to EmergeOrtho, who then provided it 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.

47. Defendant's data security obligations were particularly important given the substantial increase in data breaches, and particularly data breaches in the healthcare industry, preceding the date of the breach.

48. Data breaches, including those perpetrated against the healthcare sector of the economy, have become widespread.

49. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[16] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[17] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658),

---

[15] Eyal Benishti, How to Safeguard Hospital Data from Email Spoofing Attacks, Chief Healthcare Executive (April 4, 2019) at: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed September 7, 2022).

[16] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

[17] *Id.*

compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[18]

50. Indeed, cyberattacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

51. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[19]

52. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including EmergeOrtho.

Defendant Fails to Comply with FTC Guidelines

53. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

54. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any

---

[18] *Id.*

[19] *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 accessed September 8, 2022).

security problems.[20] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[21]

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

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

---

[20] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed September 8, 2022).
[21] *Id.*

58. Defendant failed to properly implement basic data security practices.

59. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

60. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients as outlined in its promise to comply with all federal healthcare laws. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

61. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

62. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data; and limiting which employees can access sensitive data.

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

64. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version

1.1(including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

65. These frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant's Conduct Violates HIPAA

66. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

67. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

68. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

69. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to comply with safeguards mandated by HIPAA regulations.

Defendant Breached its Obligations to Patients

70. Defendant breached its obligations to Plaintiff and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, network, and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and Data Breaches

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

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

k. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

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

m. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

n. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

o. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and

p. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

71. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

72. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

Data Breaches Put Consumers at an Increased Risk of Fraud and Identity Theft.

73. Data Breaches at medical practices such as Defendant's are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

74. For instance, loss or interruption of access to patient histories, charts, images and other information forces providers to limit or cancel patient treatment because of the disruption of service. Any interruption can lead to a deterioration in the quality of overall care patients receive at facilities affected by Data Breaches and related data breaches.

75. Data Breaches that result in the removal of protected data are also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

76. Data breaches represent a significant problem for patients who have already experienced inconvenience and disruption associated with a Data Breach.

77. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent

charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[22]

78. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

79. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

80. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

81. Theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[23] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

82. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

---

[22] *See Steps*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last accessed September 8, 2022).

[23] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

83. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

84. Where the most private information belonging to Plaintiff and Class Members was accessed and removed from Defendant's network, there is a strong probability that entire batches of stolen information have been dumped on the black market or are soon to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

85. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[24] PII, including a Social Security number, is particularly valuable because criminals can use it to target victims with frauds and scams.

86. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[25] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[26] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's

[24] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed September 8, 2022).
[25] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed September 8, 2022).
[26] *Id.* at 4.

employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

87. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[27]

88. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[28]

89. Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is $50 and up.[29] Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

90. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this risk and strengthened its data systems accordingly. Defendant

---

[27] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015. Available at http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed June 7, 2022).

[28] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed September 7, 2022).

[29] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last accessed September 7, 2022).

was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Plaintiff's Experience

91. Plaintiff Daniel Green is and was at all times relevant to this complaint an individual citizen residing in the State of North Carolina, in the City of Southport, Brunswick County. Mr. Green is and has been a patient of EmergeOrtho, which required Mr. Green to provide a variety of Private Information in order to receive treatment.

92. On or after August 25, 2022, Mr. Green received a mailed Notice Letter, related to EmergeOrtho's May 2022 Data Breach. *See* Plaintiff's Notice Letter, attached as Exhibit A.

93. The Notice Letter that Plaintiff received listed an extensive amount of his PII that was in files that "an unauthorized third part accessed" during its "sophisticated ransomeware attack." The Letter states that "it is possible that the following personal information could have been accessed by an unauthorized third party: first and last name, address, Social Security number, and in some cases, date of birth." Then it reassures him to "Please be assured that your medical records, treatment information, financial account and payment card information were not compromised . . ." Ex. A.

94. EmergeOrtho's Notice Letter oddly assures Mr. Green exactly what information was *not* compromised while concurrently being exceptionally vague about what information "could have been accessed." This Notice is far from reassuring as name, address, Social Security number, and date of birth are a cybercriminals keys to stealing a person's identity.

95. Mr. Green is alarmed by the amount of his Private Information that may have been stolen or accessed as listed on his letter, and even more by the fact that his Social Security number was identified as among the breached data on EmergeOrtho's computer system.

96. Since learning of EmergeOrtho's Data Breach, Mr. Green has been monitoring his financial accounts two or three times a day, for approximately 30 minutes each time. This time spend is far more than he spent monitoring his accounts in the past, is time he would prefer using for his own leisure and work, and is time cannot be recovered. He anticipates having to continue to closely monitor his accounts for months or years into the future as a direct result of EmergeOrtho's failure to secure its network properly.

97. As a result of EmergeOrtho' Data Breach, Mr. Green has experienced increased anxiety about the security of his Private Information.

98. Mr. Green is aware that cybercriminals often sell Private Information, and that his could be abused months or even years after this Data Breach.

99. Had Mr. Green been aware that EmergeOrtho's computer systems were not secure, he would not have entrusted EmergeOrtho with his Private Information.

Plaintiff's and Class Members' Damages

100. To date, Defendant has done absolutely nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach.

101. Moreover, EmergeOrtho has offered only a paltry one year of single bureau identity theft monitoring, with only a three-month window to enroll. This one-year, single bureau limitation offer is inadequate as it fails to provide victims of the Data Breach with any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII and PHI. Data Breach victims commonly face multiple years of ongoing identity theft and financial fraud.

102. In addition, EmergeOrtho expects Plaintiff and Class to protect themselves from its tortious acts resulting in the Data Breach. Defendant sent instructions to Plaintiff and Class

Members about actions they can affirmatively take to protect themselves, even though it failed to adhere to its own promises of protecting their Private Information.

103. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

104. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

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

106. Plaintiff and Class Members suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

107. Plaintiff and Class Members were damaged via benefit-of-the-bargain damages. Part of the price Class members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and to protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for. Specifically, they overpaid for services that were intended to be accompanied by adequate data security but were not.

108. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

109. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

110. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach.

111. In addition, many victims suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

112. Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

CLASS ACTION ALLEGATIONS

113. Plaintiff seeks relief on behalf of himself and all others similarly situated pursuant to N.C. Rule of Civil Procedure, Rule 23 as a representative of the Class defined as follows:

> All persons whose PII and/or PHI was compromised as a result of the Data Breach that EmergeOrtho discovered on or about May 1, 2022.

114. Plaintiff hereby reserves the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

115. Defendant is excluded from the Class as well as any entity in which Defendant has a controlling interest, along with Defendant's legal representatives, officers, directors, assignees and successors. Also excluded from the Class is any judge to whom this action is assigned, together with any relative of such judge, and the spouse and children of any such persons, and the members of the judge's staff and their children.

116. Numerosity. Consistent with Rule 23, the members of the Class are so numerous that the joinder of all members is impractical. The Data Breach implicates approximately **68,661** patients of EmergeOrtho, both current and former.

117. Commonality. This action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether EmergeOrtho had a duty to protect its patients' sensitive PII and PHI;

b. Whether EmergeOrtho knew or should have known of the susceptibility of its systems to a Data Breach;

c. Whether EmergeOrtho's security measures to protect its systems were reasonable considering best practices recommended by data security experts;

d. Whether EmergeOrtho was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether EmergeOrtho's failure to implement adequate data security measures allowed the breach of its data systems to occur;

f. Whether EmergeOrtho's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unlawful exposure of the Plaintiff's and Class Members' PII and PHI;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of EmergeOrtho's failure to reasonably protect its systems and data network; and,

h. Whether Plaintiff and Class Members are entitled to relief.

118. Typicality. Plaintiff's claims are typical of those of other Class Members. Plaintiff was a patient of EmergeOrtho entities who had his PII accessed and potentially exfiltrated in the Data Breach. Plaintiff's damages and injuries are akin to other Class Members, and Plaintiff seeks relief consistent with the relief sought by the Class.

119. Adequacy. Plaintiff is adequate representatives of the Class because he is a member of the Class he seeks to represent; is committed to pursuing this matter against EmergeOrtho to obtain relief for the Class; and has no conflicts of interest with the Class. Moreover, Plaintiff's attorneys are competent and experienced in litigating class actions, including privacy litigation of

this kind. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class Members' interests.

120. Superiority. 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 quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an individual Plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against EmergeOrtho, and thus, individual litigation to redress EmergeOrtho's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the 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 a single adjudication, economies of scale, and comprehensive supervision by a single court.

121. Injunctive and Declaratory Relief. Class certification is also appropriate under Rule 23. Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

122. Likewise, particular issues 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 EmergeOrtho owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII and PHI;

b. Whether EmergeOrtho's security measures to protect its data systems were reasonable considering best practices recommended by data security experts;

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

d. Whether EmergeOrtho failed to take commercially reasonable steps to safeguard employee, provider and patient PII and PHI;

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

f. Whether EmergeOrtho failed to comply with its statutory and regulatory obligations.

123. Finally, all members of the proposed Class are readily ascertainable. EmergeOrtho has access to its patients' names and addresses affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing notice.

CAUSES OF ACTION

Count I
Negligence
(On Behalf of Plaintiff and Class Members)

124. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

125. EmergeOrtho required Plaintiff and Class Members to submit non-public Private Information in order to obtain medical services.

126. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and

safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

127. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

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

129. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

130. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

131. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair

practice of failing to use reasonable measures to protect confidential data, including the Private Information accessed by cybercriminals here.

132. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

133. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to abide by its website promise of complying with all federal healthcare laws;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to have mitigation and back-up plans in place in the event of a Data Breach.

134. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

135. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

136. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach and data breach.

137. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

Count II
Invasion of Privacy
(On Behalf of Plaintiff and Class Members)

138. Plaintiff repeats and incorporates by reference each allegation in the above paragraphs as if fully set forth herein.

139. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

140. By intentionally failing to keep Plaintiff's and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and Class Members' privacy by intrusion.

141. Defendant knew that an ordinary person in Plaintiff's or a Class Member's position would consider this invasion of privacy and Defendant's intentional actions highly offensive and objectionable.

142. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

143. Defendant intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

144. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

145. Plaintiff sustained damages (as outlined above) as a direct and proximate consequence of the invasion of his privacy by intrusion, and therefore seeks an award of damages on behalf of himself and the Class.

Count III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and Class Members)

146. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

147. In providing their Private Information to Defendant, Plaintiff and Class Members justifiably placed special confidence in Defendant to act in good faith and with due regard to

interests of Plaintiff and Class Members to safeguard and keep confidential that Private Information.

148. Defendant EmergeOrtho accepted the special confidence placed in it by Plaintiff and Class Members.

149. Additionally, although Defendant acknowledges on its website to comply with federal healthcare laws, including the duty to protect Private Information, it failed to do so.

150. There was an understanding between Plaintiff and the Class Members and EmergeOrtho that Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of the Private Information.

151. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members, for the safeguarding of Plaintiff's and Class Members' Private Information.

152. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its patients' relationship, in particular, to keep secure the Private Information of its patients.

153. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach and data breach in a reasonable and practicable period of time.

154. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

155. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach and data breach.

156. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

157. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

158. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

159. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

160. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

161. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are

not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

162. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

163. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq.*

164. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

165. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

166. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

167. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity

theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach and data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach and data breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

168. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and harm, and other economic and non-economic losses.

Count IV
Breach of Implied Contract
(On Behalf of Plaintiff and Class Members)

169. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

170. Plaintiff and Class Members were required to provide their PII and PHI to Defendant as a condition of their treatment at Defendant's facilities.

171. Plaintiff and Class Members paid money to Defendant and disclosed their PII and PHI in exchange for medical services, along with Defendant's promise to protect their PII and PHI from unauthorized disclosure.

172. In its written privacy policies, Defendant EmergeOrtho promised Plaintiff and Class Members that it would only disclose PII or PHI under certain circumstances, none of which relate to the Data Breach.

173. Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII and PHI would remain protected.

174. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only; (b) take reasonable steps to safeguard that PII; (c) prevent unauthorized disclosures of the PII; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses; and (f) retain the PII only under conditions that kept such information secure and confidential.

175. When Plaintiff and Class Members provided their PII to Defendant EmergeOrtho as a condition precedent to receiving medical and surgical care, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

176. Defendant solicited, invited, and then required Class Members to provide their PII and PHI as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

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

178. Plaintiff and Class Members would not have entrusted their PII and PHI to Defendant in the absence of the implied contract between them and Defendant to keep their

information reasonably secure. Plaintiff and Class Members would not have entrusted their PII and PHI to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

179. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

180. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII and PHI.

181. As a direct and proximate result of Defendant' breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

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

183. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all Class Members.

Count V
Violation of the North Carolina Unfair and Deceptive Trade Practices Act
N.C. Gen. Stat. § 75-1.1., et seq.
(On Behalf of Plaintiff and Class Members)

184. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

185. Defendant is a North Carolina entity with headquarters in this state and is subject to the laws and regulations of the State of North Carolina, including but not limited to the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. § 75.1.1 ("UDTPA"). That

Act "declare[s] unlawful" all "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." N.C. Gen. Stat. § 75-1.1(a).

186. For purposes of North Carolina's UDTPA, the term "commerce" includes all business activities, however denominated, but does not include professional services rendered by a member of a learned profession." N.C. Gen. Stat. § 75-1.1(b).

187. Defendant violated the North Carolina UDTPA by engaging in unlawful, unfair, or deceptive business acts and practices in or affecting commerce, as well as unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" prohibited in the statute.

188. Upon information and belief, the policies, practices, acts and omissions giving rise to this action emanated from Defendant's headquarters and facilities in North Carolina.

189. Defendant engaged in unlawful acts and practices with respect to their services by establishing inadequate security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class Members' highly sensitive Private Information with knowledge that such information would not be adequately protected; and by gathering Plaintiff's and Class Members' sensitive information in an unsecure electronic environment in violation of North Carolina's data breach statute, the Identity Theft Protection Act, N.C. Gen. Stat. § 75-60, et seq., which requires Defendant to undertake reasonable methods of safeguarding the sensitive information of the Plaintiffs and other Class Members.

190. In addition, Defendant engaged in unlawful acts and practices when they failed to discover and then disclose the data security breach to Plaintiff and the Class Members in a timely and accurate manner, contrary to the duties imposed by N.C. Gen. Stat. § 75-65.

191. Defendant further violated UDTPA by violating North Carolina's Identity Theft Protection Act (ITPA), N.C. Gen. Stat. § 75-60, *et. seq.* (ITPA) by:

a. Failing to prevent the PII of Plaintiff and Class Members from falling into unauthorized hands;

b. Failing to make reasonable efforts to safeguard and protect the PII/PHI, particularly Social Security numbers, of Plaintiff and Class Members;

c. Failing to provide adequate notice of the security breach to affected patient/consumers upon discovery that their system had been compromised and PII had been disclosed; and

d. In other ways to be discovered and proven at trial.

192. Defendant willfully concealed, suppressed, omitted and failed to inform Plaintiff and Class Members of the material facts as described above.

193. As a direct and proximate result of Defendant's unlawful acts and practices, Plaintiff and Class Members have been injured, suffering ascertainable losses and lost money or property, including but not limited to the loss of their legally protected interests in the confidentiality and privacy of their sensitive information.

194. Defendant knew or should have known that their data security practices were inadequate to safeguard Plaintiff and the Class Members' Private Information, that the risk of a data security breach was significant, and that their systems were, in fact, breached.

195. Defendant's actions in engaging in the above-named unlawful practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Class Members.

196. Plaintiff and the Class Members seek relief under the North Carolina UDTPA including, but not limited to: restitution to Plaintiff and Class Members of money and property that Defendant have acquired by means of unlawful and unfair business practices; disgorgement

of all profits accruing to Defendant because of their unlawful and unfair business practices; treble damages (pursuant to N.C. Gen. Stat. § 75-16); declaratory relief; attorneys' fees and costs (pursuant to N.C. Gen. Stat. § 75-16.1); and injunctive or other equitable relief.

Count VI
Unjust Enrichment
(On Behalf of Plaintiff and Class Members)

197. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

198. Plaintiff and Class Members conferred a monetary benefit on Defendant. Part of the premiums that health plan participant Plaintiffs and Class Members paid to Defendant (or that were paid to Defendant on behalf of the health plan participant Plaintiff and Class Members) were intended to be used by Defendant to fund adequate security of Defendant's computer property and Plaintiff's and Class Members' Private Information and protect Plaintiff's and Class Members' Private Information.

199. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

200. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed

to implement appropriate data management and security measures that are mandated by industry standards.

201. Defendant acquired the PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

202. If Plaintiff and Class Members knew that Defendant had not secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant EmergeOrtho.

203. Plaintiff and Class Members have no adequate remedy at law.

204. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity to direct how their PII and PHI are used; (c) the compromise, publication, and/or theft of their PII and PHI; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII and PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and PHI in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

205. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

206. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

207. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays 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;

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

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 PII and PHI compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

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

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this Complaint so triable. Plaintiff also respectfully requests leave to amend this Complaint to conform to the evidence, if such amendment is needed for trial.

Dated: September 12, 2022

Respectfully Submitted,

Scott C. Harris with permission Scott E. Holdren

Scott C. Harris
N.C. State Bar: 38328
Milberg Coleman Bryson Phillips Grossman PLLC
900 W. Morgan St.
Raleigh, NC 27603
Phone: 919-600-5000
Fax: 919-600-5035
sharris@milberg.com

Gary M. Klinger*
Milberg Coleman Bryson Phillips Grossman PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Raleigh, NC 27603
Phone: 866-252-0878
gklinger@milberg.com

Gary E. Mason
Danielle L. Perry*
Lisa A. White
MASON LLP
5101 Wisconsin Ave. NW Ste. 305
Washington DC 20016
Phone: 202.640.1160
Fax: 202.429.2294
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Attorneys for Plaintiff and the Class

**pro hac vice forthcoming*

EXHIBIT A

EmergeOrtho
c/o Cyberscout
38120 Amrhein Road
Livonia, MI 48150

[redacted]
DANIEL GREEN
[redacted]
SOUTHPORT, NC 28461 [redacted]
[redacted]

EmergeOrtho

2716 Ashton Drive
Wilmington, NC 28412

POLXN70U2...

August 25, 2022

Notice of Data Security Incident

Dear Daniel Green,

EmergeOrtho is an orthopedic practice serving five regions across North Carolina. We are writing to inform you of an incident that involved your personal information. We take the security of your personal information seriously, and want to provide you with information and resources you can use to protect your information.

What Happened and What Information was Involved:

On May 18, 2022, we detected and stopped a sophisticated ransomware attack, in which an unauthorized third party accessed some of EmergeOrtho's computer systems. We immediately engaged a third-party forensic firm to assist us with securing the network environment and investigating the extent of any unauthorized activity. The investigation concluded on August 19, 2022. Our investigation determined that an unauthorized third party accessed certain individual personal information during this incident.

We found no evidence that your information has been specifically misused; however, it is possible that the following personal information could have been accessed by an unauthorized third party: first and last name, address, Social Security number, and, in some cases, date of birth. Please be assured that your medical records, treatment information, financial account and payment card information were not compromised as a result of this incident.

What We Are Doing:

Data security is one of our highest priorities. Upon detecting this incident we moved quickly to initiate a response, which included retaining a leading forensic investigation firm who assisted in conducting an investigation along with the assistance of leading IT specialists to confirm the security of our network environment. Additionally, we are coordinating with the FBI We have also deployed additional monitoring tools and will continue to enhance the security of our systems.

We value the safety of your personal information and are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score* services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have, or in the event your identity is compromised. These services will be provided by CyberScout through Identity Force, a company specializing in fraud assistance and remediation services..

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/emergeortho** and follow the instructions provided. When prompted please provide the following unique code to receive services [redacted] Please note the deadline to enroll is **November 30, 2022.**

The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We encourage you to take full advantage of this service offering. The call center representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

If you have additional questions, please call the dedicated call center at 1-833-514-2246, Monday through Friday, 8:00am - 8:00pm Eastern time, excluding holidays. Representatives are available for 90 days

Sincerely,

Allison Farmer, CEO
EmergeOrtho

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
https://www.equifax.com/personal/credit-report-services/credit-freeze/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
https://www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (https://www.transunion.com/fraud-alerts); or
- Experian (https://www.experian.com/fraud/center.html).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at listed above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and https://ag.ny.gov/.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).