CAUSE NO. DC-24-00843

EFSTATHIOS MAROULIS, BRUCE DAY, and RUBY MORAN, individually and on behalf of all others similarly situated,	§	IN THE DISTRICT COURT
Plaintiffs,	§	
v.	§	44TH JUDICIAL DISTRICT
COOPER CLINIC, P.A., COOPER MEDICAL IMAGING, LLP, and COOPER AEROBICS ENTERPRISES, INC.,	§	
Defendant.		DALLAS COUNTY, TEXAS

PLAINTIFFS' AMENDED CLASS ACTION PETITION

TO THE HONORABLE JUDGE OF SAID COURT:

COME NOW, Plaintiffs Efstathios Maroulis, Bruce Day, and Ruby Moran, individually and on behalf of all others similarly situated, upon personal knowledge of all facts pertaining to themselves and on information and belief as to all other matters, by and through the undersigned counsel, bring this Class Action Complaint against Defendants Cooper Clinic, P.A., Cooper Medical Imaging, LLP, and Cooper Aerobics Enterprises, Inc. (collectively, "Defendants").

I. NATURE OF THE ACTION

1. Plaintiffs bring this action, individually and on behalf of all others similarly situated, private and confidential personal identifying information ("PII") and/or protected health information ("PHI")—including their name, Social Security numbers, drivers' license numbers, financial account information, protected health information, EIN/Tax Identification Numbers, and

dates of birth—was compromised in a massive security breach of Defendants' computer servers (the "Data Breach").

2. As alleged herein, Defendants' failure to implement adequate data security measures to protect its consumers' sensitive PII/PHI and proximately caused injuries to Plaintiffs and the class members.

3. The Data Breach was the inevitable result of Defendants' inadequate data security measures and cavalier approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving PII/PHI, Defendants failed to ensure that it maintained adequate data security measures to protect PII/PHI from unauthorized third parties.

4. By collecting, using, and deriving a benefit from the PHI of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. Defendants had legal obligations and duties created by HIPAA, contract, industry standards, common law, and representations made to Class Members, to keep Class Members' PII/PHI confidential and to protect it from unauthorized access and disclosure.

6. Defendants failed to adequately protect Plaintiffs' and Class Members' PII/PHI and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PHI was compromised due to Defendants' negligent and/or careless acts and omissions and its utter failure to protect the sensitive data it collected for its own pecuniary gain.

7. Had Defendants adequately designed, implemented, and monitored its network and servers, the Data Breach would have been prevented.

8. Had Plaintiffs and Class Members known that Defendants' data security was below industry standards, Plaintiffs and Class Members would not have provided their PII/PHI to Defendants or relied on Defendants to protect that information.

9. As a result of Defendants' inadequate data security practices that resulted in the Data Breach, Plaintiffs and Class Members are at an imminent risk of identity theft and have suffered numerous actual and concrete injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain; (d) diminution of value of their PII/PHI; (e) the continued risk to their health; and (f) the continued risk to their PII/PHI, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII/PHI.

10. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII/PHI.

11. Defendants failed to offer any meaningful assistance to consumers to help deal with the fraud that has and will continue to result from the Data Breach. In contrast to what has been frequently made available to consumers in other data breaches, Defendants have not offered or provided any fraud insurance.

12. Despite discovering the Data Breach in February of 2023, Defendants inexplicably failed to provide notice to impacted customers until January 5, 2024. As a result, Defendants left a significant gap of time in which, unbeknownst to its customers, Defendants knew of and could have notified its customers of the Data Breach and advised its customers to take immediate remedial steps. Instead, Defendants left its customers exposed.

13. Plaintiffs and Class Members seek to recover damages caused by Defendants' negligence, negligence per se, breach of fiduciary duty, breach of implied contract, and unjust enrichment. Additionally, Plaintiffs seek declaratory and injunctive relief as a result of Defendants' conduct, as discussed herein.

II. PARTIES

14. Plaintiff Efstathios Maroulis is an individual residing in Dallas County, Texas.

15. Plaintiff Bruce Day is an individual residing in Oklahoma.

16. Plaintiff Ruby Moran is an individual residing in Grayson County, Texas.

17. Defendant Cooper Clinic, P.A. ("Cooper Clinic") is a professional association organized and existing under the laws of the State of Texas. Cooper Clinic's principal office is located in Dallas County, Texas. Cooper Clinic has already appeared in this lawsuit through counsel of record.

18. Defendant Cooper Medical Imaging, LLP ("Cooper Medical") is a limited liability company organized and existing under the laws of the State of Texas. Cooper Medical's principal office is located in Dallas County, Texas. Cooper Medical has already appeared in this lawsuit through counsel of record.

19. Defendant Cooper Aerobics Enterprises, Inc. ("Cooper Aerobics") is a domestic corporation organized and existing under the laws of the State of Texas. Cooper Aerobics' principal office is located in Dallas County, Texas. Cooper Aerobics has already appeared in this lawsuit through counsel of record.

III. JURISDICTION & VENUE

20. This Court has subject matter jurisdiction, as the amount in controversy exceeds the minimum jurisdictional limits of this Court.

21. Venue is proper in Dallas County, Texas pursuant to Texas Civil Practice & Remedies Code § 15.002(a)(3), as Dallas County is the county of Defendants' principal offices in the State of Texas.

IV. FACTS

22. Plaintiffs and the proposed Class are consumers of Cooper Clinic, P.A., Cooper Medical Imaging, LLP, and/or Cooper Aerobics Enterprises, Inc. Cooper Aerobics is a prominent health and wellness center, which includes the Cooper Clinic, P.A., and Cooper Medical Imaging, LLP.

23. As noted above, Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard PII/PHI, for failing to comply with industry standards to protect and safeguard that information, and for failing to provide timely, accurate, and adequate notice to Plaintiffs and other members of the class that such information has been compromised.

A. Cooper Defendants were obligated to safely protect its consumers' PII/PHI.

24. Plaintiffs' and Class Members' PII/PHI was provided to Cooper Defendants in conjunction with the type of work Cooper Defendants do in providing health and wellness services. Upon information and belief, as a condition of providing its services to its customers, Defendants required that each customer sign a form authorizing the use and/or disclosure of their protected health information, pursuant to HIPAA.

25. Plaintiffs and Class Members provided their PII/PHI to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

26. In receiving the PII/PHI as part of its services, Defendants assented and undertook legal duties to safeguard and protect the PII/PHI entrusted to them by Plaintiffs and Class Members, in compliance with all applicable laws, including HIPAA.

27. These duties included the obligation to mitigate cybersecurity risks and enhance data breach resilience through a tailored cybersecurity program. This required Defendants to, at very least, perform a risk assessment to identify areas for improvement and to provide security responses and recommended controls for each stage of a ransomware attack, including phishing prevention, multi-factor authentication, endpoint detection and response, and network segmentation.

28. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting medical facilities preceding the date they disclosed the incident. According to the 2023 State of Ransomware in Healthcare report by Sophos, 66% of surveyed healthcare organizations fell victim to a ransomware attack in 2023; and ransomware is arguably the biggest cyber risk facing the healthcare sector today.[1]

29. 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."[2]

30. 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

---

[1] *The State of Ransomware in Healthcare in 2023*, SOPHOS (Aug. 2023) (last accessed Oct. 17, 2023), *available at* https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-healthcare.

[2] 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.

ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[3]

31. Defendants were on notice that the FBI has recently been concerned about data security regarding entities that store certain amounts of PHI, as Defendants do. 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)."[4]

32. However, Defendants ignored these warnings and failed to ensure security for the PHI of the individuals that provided them with this sensitive information. Its loose data protection policies and practices left its patients' data exposed.

B. The Data Breach exposed thousands of patients' PHI.

33. According to Copper Defendants notice, in February of 2023, it was notified of a cyber incident.

34. Defendants were not forthcoming about any specifics. In Plaintiffs' Notice of Data Security Incident, dated January 8, 2024, Defendants merely identified that name, medical information, and health insurance information was subjected to the attack.

35. Moreover, Defendants did not reveal the details or the root cause of the Data Breach, the vulnerabilities exploited, whether Defendants' system is still unsecured, or any

[3]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.

[4]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.

remedial measures Defendants were taking to ensure such a breach does not occur again. Defendants still have not explained or clarified these details to Plaintiffs or the Class Members who have a vested interest in ensuring that their PII/PHI remains protected.

36. However, according to the Dallas Morning News, the Defendants' Data Breach was far more injurious than Defendants admitted: it resulted in a successful infiltration of the company's extensive database containing nearly 90,000records.[5]

37. The leaked data reportedly included a vast range of sensitive information such as health information, dates of birth, credit debit card numbers, financial accounts, routing information, tax identification information, drivers licenses, government IDs, passport and social security numbers.

38. Defendants failed to take appropriate or even the most basic steps to protect the PII/PHI of Plaintiffs and other Class Members from being disclosed. Upon information and belief, Defendants failed to adequately perform a risk assessment to identify areas for improvement or put in place adequate security responses, phishing prevention, multi-factor authentication, endpoint detection and response, or network segmentation.

39. Further, upon information and belief, the PII/PHI contained in the files accessed by cybercriminals was not encrypted or inadequately encrypted, as the threat actors were able to acquire and steal Plaintiffs' and Class Members' PII/PHI.

40. Defendants allegedly reported this data breach to the Texas Attorney General as required by Texas law. Texas law specifically requires that any business that experiences a data breach "notify the attorney general of that breach not later than the 30th day after the date on which

---

[5]Paul O'Donnell, *Data breach at Dallas-based Copper Aerobics exposes 90,000 customer accounts,* The Dallas Morning News (Jan. 17, 2024) /.

the person determines that the breach occurred if the breach involves at least 250 [Texas] residents." Tex. Bus. & Com. Code Ann. § 521.053.

C. Plaintiffs and the Class Members have suffered as a result of the Data Breach.

41. Personally Identifying Information ("PII") is a valuable property right.[6] Its value as a commodity is measurable.[7] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[8] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[9] 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.

42. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] 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 fetch up to

---

[6] *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 and preferences as possible...").

[7] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited January 16, 2023).

[8] *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.

[9] 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/.

[10] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

$1,200 to $1,300 each on the black market.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

43. Stolen PHI is one of the most valuable commodities on the criminal information black market. According to both a report released by the Federal Bureau of Investigation's Cyber Division[13] and ClearDATA Chief Privacy and Security Officer and Founder Chris Bowen, a medical record is 50 times more valuable than a credit card number.[14] As Mr. Bowen explains: "[i]t is not just the credit card. You can build an entire persona around a health record. You can create or seek medical treatment, abuse drugs, or get prescriptions. The lifespan is so much longer than a credit card."[15]

44. Moreover, according to the National Association of Healthcare Access Management, stolen PHI can result in medical identity theft which can pose a threat to not just a person's finances, but also their health – it has been referred to "the privacy crime that can kill."[16]Thieves have the potential to alter personal medical records, including blood type, allergies, or medicine, which can have a potentially fatal outcome.[17]

---

[11]Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[12]*In the Dark*, VPNOverview.com, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on January 16, 2023).

[13]*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.

[14]Will Maddox, *Why Medical Data is 50 Times More Valuable Than a Credit Card*, D. Magazine (Oct. 15, 2019) (last accessed Oct. 17, 2023), *available at* https://www.dmagazine.com/healthcare-business/2019/10/why-medical-data-is-50-times-more-valuable-than-a-credit-card/.

[15]Id.

[16]Laurie Zabel, CHC, CPC, *The Value of Personal Medical Information: Protecting Against Data Breaches*, National Association of Healthcare Access Management (last accessed Oct. 17, 2023), *available at* https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information.

[17]Id.

45. Moreover, criminals can use stolen PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[18] 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."[19]

46. It can take victims years to spot or identify PHI theft and is easily concealed, giving criminals plenty of time to milk that information for cash. Only ten (10) percent of victims report receiving a satisfactory resolution to their stolen PHI, and those who found a resolution spent more than 200 working hours to do so.[20]

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

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

49. Plaintiffs 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

---

[18] *See* https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.

[19] Id.

[20] Zabel, *supra* n.16.

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

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.

50. 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, Plaintiffs and the Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendants' conduct. Further, the value of Plaintiffs' and Class Members' PHI has been diminished by its exposure in the Data Breach.

51. As a result of Defendants' failures, Plaintiffs and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their PHI.

52. Plaintiffs and the Class Members suffered actual injury from having PII/PHI compromised as a result of the Cooper Defendants' negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII/PHI, a form of property that Defendants' obtained from Plaintiffs; (b) violation of their privacy rights; (c) present and increased risk arising from the identity theft and fraud; (d) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (e) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; and (f) invasion of privacy.

53. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiffs and members of the Class these significant injuries and harm.

54. Plaintiffs bring this class action against the Cooper Defendants for their failure to properly secure and safeguard PII/PHI and for failing to provide timely, accurate, and adequate notice to Plaintiffs and other Class Members that their PHI had been compromised.

V. CLASS ALLEGATIONS

55. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose PHI was compromised in the Data Breach occurring in February of 2023, including all individuals to whom Cooper Clinic, P.A., Cooper Medical Imaging, LLP, and/or Cooper Aerobics Enterprises, Inc. mailed notice to on or around January/February of 2024.

56. Excluded from the Class are Defendants' officers and directors, and any entity in which Cooper Clinic, Cooper Medical and/or Cooper Aerobics have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Cooper Clinic, Cooper Medical and/or Cooper Aerobics. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

57. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

58. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. As noted above, there are approximately 90,000 Members.

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

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII/PHI;

b. Whether Defendants 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 Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

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

e. Whether Defendants owed a duty to Class Members to safeguard their PII/PHI;

f. Whether Defendants breached their duty to Class Members to safeguard their PII/PHI;

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

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

i. Whether Defendants' conduct was negligent;

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

k. Whether Defendants' acts breaching an implied contract they formed with Plaintiffs and the Class Members;

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

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

n. Whether Defendants were unjustly enriched to the detriment of Plaintiffs and the Class;

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

and

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

60. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII/PHI, like that of every other Class Member, was compromised in the Data Breach.

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

62. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' 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.

63. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. 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.

64. Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

65. 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 Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, using, and safeguarding their PII/PHI;

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

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

d. Whether Defendants 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.

66. Finally, all members of the proposed Class are readily ascertainable. Defendants have 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 Defendants.

VI. CAUSES OF ACTION

A. Count I - Negligence

67. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

68. Defendants owed a duty to Plaintiffs and all other Class Members to exercise reasonable care in safeguarding and protecting the PII/PHI in their possession, custody, or control.

69. Defendants knew, or should have known, the risks of collecting and storing Plaintiffs' and all other Class Members' PII/PHI and the importance of maintaining secure systems. Defendants knew, or should have known, of the vast uptick in data breaches in recent years. Defendants had a duty to protect the PII/PHI of Plaintiffs and Class Members.

70. Given the nature of Defendants' business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Defendants should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Defendants had a duty to prevent.

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

72. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would

result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' PHI to unauthorized individuals.

73. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiffs and Class Members, their PII/PHI would not have been compromised.

74. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs 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 PII/PHI; (iii) breach of the confidentiality of their PHI; (iv) deprivation of the value of their PII/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.

B. Count II – Negligence Per Se

75. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

76. Defendants' duties arise from, in part due to its storage of certain medical information, 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").

77. Defendants' 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 Defendants, of failing to employ reasonable measures to protect and secure PHI.

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

79. Defendants are an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

80. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class Members' PHI and not complying with applicable industry standards. Defendants' 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 Plaintiffs and the other Class Members.

81. Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitute negligence per se.

82. Plaintiffs 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.

83. The harm occurring because 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.

84. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class Members' PHI to unauthorized individuals.

85. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Defendants' 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.

C. Count III – Breach of Fiduciary Duty

86. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

87. Plaintiffs and Class Members either directly or indirectly gave Defendants their PII/PHI in confidence, believing that Defendants – healthcare and wellness providers – would protect that information. Plaintiffs and Class Members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiffs' and Class Members' PII/PHI created a fiduciary relationship between Defendants and Plaintiffs and Class Members. In light of this relationship, Defendants must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

88. Defendants have a fiduciary duty to act for the benefit of Plaintiffs 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 Plaintiffs' and Class Members' PII/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.

89. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiffs 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 PI/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI/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 Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PI/PHI compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

D. Count IV – Unjust Enrichment

90. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

91. Plaintiffs and Class Members conferred a monetary benefit upon Defendants in the form of monies paid for healthcare services or other services.

92. Defendants accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Defendants also benefitted from the receipt of Plaintiffs' and Class Members' PHI.

93. As a result of Defendants' conduct, Plaintiffs 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 Plaintiffs and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

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

95. Defendants should be compelled to provide for the benefit of Plaintiffs and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

E. Count V – Breach of Implied Contract

96. Plaintiffs reallege and incorporate by reference all allegations of the preceding factual allegations as though fully set forth herein.

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

98. Plaintiffs and Class Members would not have provided their PII/PHI to Defendants had they known that Defendants would not safeguard their PII/PHI, as promised, or provide timely notice of a data breach.

99. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendants.

100. Defendants breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PHI and by failing to provide them with timely and accurate notice of the Data Breach.

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

VII. JURY DEMAND

102. Plaintiffs demand a jury trial and have previously tendered the appropriate fee to this Court.

VIII. PRAYER

WHEREFORE, Plaintiffs, individually and on behalf of the Class, pray for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

b. For equitable relief enjoining Cooper Clinic, Cooper Medical and/or Cooper Aerobics from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII/PHI;

c. For equitable relief compelling Cooper Clinic, Cooper Medical and/or Cooper Aerobics to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII/PHI compromised during the Data Breach;

d. For an order requiring Cooper Clinic, Cooper Medical and/or Cooper Aerobics to pay for credit monitoring services for Plaintiffs and the Class of a duration to be determined at trial;

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.

Dated: April 11, 2024

Respectfully submitted,

By: /s/*Bruce W. Steckler*

Bruce W. Steckler
TX Bar No. 00785039
bruce@swclaw.com
Paul D. Stickney, of Counsel
TX Bar No. 00789924
judgestick@gmail.com
STECKLER WAYNE & LOVE, PLLC
12720 Hillcrest Road, Suite 1045
Dallas, TX 75230
Tel: (972) 387-4040
Fax: (972) 387-4041

John A. Yanchunis
TX Bar No. 22121300
jyanchunis@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, Florida 33602
T: (813) 223-5505
F: (813) 223-5402

William B. Federman
TX Bar No. 00794935
wbf@federmanlaw.com
FEDERMAN & SHERWOOD
212 W. Spring Valley Road
Richardson, TX 75081
Telephone: (214) 696-1100
Facsimile: (214) 740-0112

Gary M. Klinger
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606

Phone: (866) 252-0878
gklinger@milberg.com

ATTORNEYS FOR PLAINTIFFS AND THE PROPOSED CLASS

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing document was served on all counsel pursuant to the Texas Rules of Civil Procedure on April 11, 2024.

/s/ Bruce W. Steckler
Bruce W. Steckler

Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Jamie Baciak on behalf of Bruce Steckler
Bar No. 785039
jamie@swclaw.com
Envelope ID: 86573452
Filing Code Description: Amended Petition
Filing Description: PLAINTIFFS'
Status as of 4/12/2024 10:06 AM CST

Associated Case Party: EFSTATHIOS MAROULIS

Name	BarNumber	Email	TimestampSubmitted	Status
Bruce WilliamSteckler		bruce@swclaw.com	4/11/2024 4:36:12 PM	SENT
Jamie Baciak		jamie@swclaw.com	4/11/2024 4:36:12 PM	SENT
Austin PSmith		austin@swclaw.com	4/11/2024 4:36:12 PM	SENT
Robyn Shiplet		Robyn@swclaw.com	4/11/2024 4:36:12 PM	SENT

Associated Case Party: COOPER CLINIC, P.A.

Name	BarNumber	Email	TimestampSubmitted	Status
Noah Nadler		noah.nadler@wickphillips.com	4/11/2024 4:36:12 PM	SENT
Shelby Broaddus		shelby.broaddus@wickphillips.com	4/11/2024 4:36:12 PM	SENT
Jaime Olson		jaime.olson@wickphillips.com	4/11/2024 4:36:12 PM	SENT
Katy Dinsmore		katy.dinsmore@wickphillips.com	4/11/2024 4:36:12 PM	SENT