UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

Desiree McCormick, on behalf of herself and all others similarly situated 1155 Ripley St., Apt 720 Silver Spring, MD 20910, Plaintiff, v. **THE RETINA GROUP OF WASHINGTON, PLLC A/K/A THE RETINA GROUP OF WASHINGTON, LLC** 7501 Greenway Center Dr., Ste. 300 Greenbelt, MD 20770, Defendant.	Case No. CLASS ACTION COMPLAINT **JURY TRIAL DEMANDED**

Plaintiff Desiree McCormick, individually and on behalf of all similarly situated persons, allege the following against Defendant The Retina Group of Washington, PLLC a/k/a The Retina Group of Washington, LLC ("Defendant") based upon personal knowledge and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") resulting from Defendant's failure to implement reasonable and industry standard data security practices.

2. Defendant is a retinal and macular care practice with seventeen locations, serving the Washington metropolitan area for almost fifty years. and, in course of providing those services,

collected and maintained certain personally identifiable information of Plaintiff and the putative Class Members (defined below), who are (or were) patients at Defendant and/or a healthcare entity that contracted with Defendant for the provision of services.

3. Plaintiff and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

4. The information compromised in the Data Breach included Plaintiff's and Class Members' full names, addresses, email, dates of birth, Social Security numbers, driver's license, ("personally identifiable information" or "PII") and medical and health insurance information, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

5. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who targeted the Private Information for its value to identity thieves.

6. As a result of the Data Breach, Plaintiff and Class Members suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) an increase in spam calls, texts, and/or emails; (viii) Plaintiff Brent's and Plaintiff Dike's Private Information being disseminated on the dark web; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains

backed up 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.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its patients' and its clients' patients' Private Information from a foreseeable and preventable cyber-attack.

8. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff and Class Members' Private Information was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

9. Defendant disregarded the rights of Plaintiff and Class Members by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

10. Plaintiff and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future 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' 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.

12. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent 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.

13. Plaintiff and Class Members may also incur out of pocket costs, e.g., for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

15. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

16. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

II. PARTIES

17. Plaintiff Desiree McCormick is, and at all times mentioned herein was, an individual citizen of the State of Maryland.

18. Plaintiff's information was stored with Defendant as a result of her dealings with Defendant. She is a current patient and treats annually with Defendant, having last been there in September 2023.

19. As required in order to obtain services from Defendant, Plaintiff provided Defendant with highly sensitive health, personal, and financial information, who then possessed and controlled it.

20. As a result, Plaintiff's information was among the data accessed by an unauthorized third-party in the Data Breach.

21. At all times herein relevant, Plaintiff is and was a member of the Class. She received a letter from the Defendant on December 22, 2023. *See* Notice Letter, attached hereto as **Exhibit A.**

22. As a result, Plaintiff was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring their accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

23. Plaintiff has also experienced an increased number of spam and suspicious calls, emails and text messages following the Data Breach and believes that these may be phishing attempts designed to gain access to additional personal information.

24. Plaintiff was also injured by the material risk to future harm suffered based on Defendant's breach; this risk is imminent and substantial because Plaintiff's data has been exposed in the breach, the data involved, including Social Security numbers and healthcare information, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's clientele, that some of the Class's information that has been exposed has already been misused.

25. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information—a condition of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

26. Plaintiff, as a result of the Data Breach, has increased anxiety for their loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling her Private Information and financial information.

27. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information and financial information, in combination with her name, being placed in the hands of unauthorized third parties/criminals.

28. As this information was among those accessed in the Data Breach, it is very likely more of her information – including highly sensitive material like Social Security numbers – are now also on the dark web.

29. Plaintiff has a continuing interest in ensuring that her Private Information and financial information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

30. Plaintiff would not have provided her Private Information to Defendant had she known of its lax security measures.

31. Defendant **The Retina Group of Washington**, PLLC a/k/a The Retina Group of Washington, LLC, is a Virginia limited liability corporation headquartered at 7501 Greenway Center Drive, Suite 300, Greenbelt, MD 20770.

III. JURISDICTION AND VENUE

32. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from Defendant.

33. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. §1367.

34. Defendant is headquartered and routinely conducts business in the State where this district is located, has sufficient minimum contacts in this State, and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

35. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims occurred within this District, and Defendant does business in this Judicial District.

IV. FACTUAL ALLEGATIONS

A. *Defendant's Business and The Data Breach*

36. Defendant provides healthcare services.

37. In the course of their relationship, patients at Defendant and/or Defendant's clients, including Plaintiff and Class Members, provided Defendant, directly or indirectly, with at least the

following information: names, dates of birth, addresses, emails, Social Security numbers, health insurance information, and medical treatment and/or diagnosis information.

38. At all relevant times, Defendant knew or should have known, that Plaintiff and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PHI/PII and financial information.

39. On no later than March 26, 2023, upon information and belief, unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PHI/PII and financial information as hosted with Defendant, with the intent of engaging in the misuse of the PHI/PII and financial information, including marketing and selling Plaintiff's and Class Members' PHI/PII and financial information.

40. The total number of individuals who have had their data exposed due to Defendant's failure to implement appropriate security safeguards is approximately 456,000 individuals.

41. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as a healthcare entity service provider that collects, creates, and maintains its patients' and its clients' patients' Private Information on its computer networks and/or systems.

42. The files containing Plaintiff's and Class Members' Private Information that were targeted and stolen from Defendant.

43. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendant that included the Private Information of Plaintiff and Class Members.

44. As evidenced by the Data Breach's occurrence, the Private Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

45. Plaintiff's Private Information was accessed and stolen in the Data Breach.

46. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

47. Defendant had obligations created by the FTC Act, HIPAA, contract, state and federal law, common law, and industry standards to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

B. *Data Breaches Are Preventable*

48. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

49. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

50. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[1]

51. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, patients and individuals should be aware of the threat of ransomware and how it is delivered.

[1] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited January 14, 2024).

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[2]

52. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

[2] *Id.* at 3-4.

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[3]

53. Given that Defendant were storing the sensitive Private Information of its current and former patients as well as its clients' current and former patients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

54. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiff and Class Members.

C. *Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Private Information*

55. Defendant acquires, collects, and stores Private Information in the regular course of its business.

56. As a condition of obtaining medical services or products at Defendant and/or its clients, Defendant requires that patients, former patients, and other personnel—including Plaintiff and Class Members—entrust it with highly sensitive personal information.

57. By obtaining, collecting, and using Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

58. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

---

[3] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited January 14, 2024).

59. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

D. *Defendant Knew or Should Have Known of the Risk Because Healthcare Entities in Possession of Private information Are Particularly Suspectable To Cyber Attacks*

60. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendant, preceding the date of the breach.

61. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread.

62. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[4]

63. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

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

64. Indeed, cyber-attacks, 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. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[5]

65. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

66. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

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

68. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—

[5] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?n1_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=news1etter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

E. *Value of Private Information*

69. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[6] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[7]

70. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[8]

71. For example, Personal Information can be sold at a price ranging from $40 to $200.[9] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[10]

72. For example, Social Security numbers are among the worst kind of Private

[6] 17 C.F.R. § 248.201 (2013).

[7] *Id.*

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).

[9] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).

[10] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).

Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[11]

73. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

74. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[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."[12]

75. Theft of PHI is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get

[11] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 17, 2022).

[12] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Oct. 17, 2022).

other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[13]

76. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[14]

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

78. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[15]

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

80. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also

---

[13] *What To Know About Medical Identity Theft,* Federal Trade Commission, (May 2021), *available at* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Aug. 3, 2023).

[14] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021)

[15] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 17, 2022).

between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

81. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

F. *Defendant Fails to Comply with FTC Guidelines*

82. 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.

83. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These 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 security problems.[17]

---

[16] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

[17] *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 visited Oct. 17, 2022).

84. 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.[18]

85. The FTC further recommends that companies not maintain Private Information 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.

86. 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.

87. These FTC enforcement actions include actions against healthcare entities, 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.").

88. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice

[18] *Id.*

by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

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

90. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

91. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its patients' and its clients' patients. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

G. ***Defendant Fails to Comply with HIPAA Guidelines***

92. Defendant is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and 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.

93. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[19] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

94. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

95. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

96. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

97. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

98. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

[19] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

99. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

100. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

101. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[20]

102. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the

[20] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

103. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

104. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[21] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[22]

H. *Defendant Fails to Comply with Industry Standards*

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

---

[21] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

[22] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

106. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

107. 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. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

108. Defendant failed to meet the minimum standards of any of the following 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 all established standards in reasonable cybersecurity readiness.

109. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and upon information and belief, Defendant failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

I. *COMMON INJURIES & DAMAGES*

110. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) loss of time due to increased spam and targeted marketing emails; (e) the loss of benefit of the bargain (price premium damages); (f) diminution of value of their Private Information; and (g) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

J. *The Data Breach Increases Victims' Risk of Identity Theft*

111. The unencrypted Private Information of Class Members will end up for sale on the dark web, as that is the *modus operandi* of hackers.

112. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Simply, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

113. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other

criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

114. Plaintiff's and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

115. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

116. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

117. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[23]

[23] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials

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

119. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

120. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

121. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

---

associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm,* Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance- finn/ (last visited on May 26, 2023).

K. *Loss of Time to Mitigate the Risk of Identity Theft and Fraud*

122. As a result of the recognized risk of identity theft, when a Data Breach occurs, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

123. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, monitor their financial accounts for many years to mitigate the risk of identity theft.

124. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, contacting financial institutions to ensure their financial accounts are secured, exploring credit monitoring and identity theft insurance options, seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach, researching how best to ensure that they are protected from identity theft, reviewing account statements and other information for any indication of fraudulent activity, which may take years to detect.

125. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[24]

[24] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

126. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach 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 seven 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.[25]

L. *Diminution of Value of PII and PHI*

127. PII and PHI are valuable property rights.[26] Their 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.

128. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[27]

129. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[28] In fact, the data marketplace is so

---

[25] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

[26] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

[27] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, 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).

[28] *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 visited Sep. 13, 2022).

sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[29,30] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[31]

130. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

131. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

132. The fraudulent activity resulting from the Data Breach may not come to light for years.

133. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information .

[29] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[30] https://datacoup.com/

[31] https://digi.me/what-is-digime/

134. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

M. *Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary*

136. Given the type of targeted attack in this case, sophisticated criminal activity, the type of Private Information involved, the volume of Private Information impacted in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

137. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or his Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

138. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

139. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class

Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

N. *Loss of Benefit of the Bargain*

140. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or Defendant's clients for medical services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service that provided the necessary data security to protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant and/or Defendant's clients.

V. CLASS ACTION ALLEGATIONS

141. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themself and the following Class:

> All individuals whose PHI/PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach experienced by Defendant.

142. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

143. Plaintiff reserves the right to modify or amend the definitions of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

144. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

145. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

146. 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 Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA and/or HIPAA;

c. When Defendant learned of the Data Breach;

d. Whether Defendant's response to the Data Breach was adequate;

e. Whether Defendant unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

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

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

i. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

j. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

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

o. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

p. Whether Defendant's conduct was negligent;

q. Whether Defendant's conduct was *per se* negligent;

r. Whether Defendant was unjustly enriched;

s. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

147. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories for all Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

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

150. Superiority. A Class action is superior to other available methods 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. 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 Defendant. In contrast, conducting 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.

151. Defendant has also acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

152. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

VI. CLAIMS FOR RELIEF

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

153. Plaintiff restates and reallege all of the allegations stated above as if fully set forth herein.

154. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

155. Defendant knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Defendant was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

156. Defendant owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Defendant's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

157. Defendant's duty to employ reasonable data security measures arose, in part, 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.

158. Defendant's duty also arose because Defendant was bound by industry standards to protect its patients' and its clients' patients' confidential Private Information.

159. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Defendant owed them a duty of care to not subject them to an unreasonable risk of harm.

160. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

161. Defendant, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

162. Defendant, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

163. 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 email system maintained reasonable data security safeguards;

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

e. Failing to comply with the FTCA and/or HIPAA.

164. Defendant had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Defendant with their Private Information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems (and the Private Information that it stored on them) from attack.

165. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.

166. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding exactly what Private Information has been compromised, Plaintiff and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

167. Defendant's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

168. As a result of Defendant's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

169. Defendant also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

170. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

171. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

172. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

173. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

174. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

175. Through its course of conduct, Defendant, Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PHI/PII and financial information.

176. Defendant required Plaintiff and Class Members to provide and entrust their PHI/PII and financial information as a condition of obtaining Defendant's services.

177. Defendant solicited and invited Plaintiff and Class Members to provide their PHI/PII and financial information as part of Defendant's regular business practices.

178. Plaintiff and Class Members accepted Defendant's offers and provided their PHI/PII and financial information to Defendant.

179. As a condition of their relationship with Defendant, Plaintiff and Class Members provided and entrusted their PHI/PII and financial information to Defendant.

180. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

181. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PHI/PII and financial information to Defendant, in exchange for, amongst other things, the protection of their PHI/PII and financial information.

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

183. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and financial information and by failing to provide timely and accurate notice to them that their PHI/PII and financial information was compromised as a result of the Data Breach.

184. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

185. Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

186. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

187. This Count is pleaded in the alternative to the breach of implied contract claim (Count II) above.

188. Plaintiff and Class Members conferred a benefit on Defendant by turning over their valuable Private Information to Defendant in exchange for cybersecurity measures sufficient to protect their Private Information from unauthorized access and disclosure. Plaintiff and Class Members did not receive such protection.

189. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including from payments made to it by or on behalf of Plaintiff and Class Members.

190. As such, a portion of these payments made to Defendant is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

191. Defendant has retained the benefits of its unlawful conduct, including the amounts of payment received from or on behalf of Plaintiff and Class Members, which payment should have been used for adequate cybersecurity practices that it failed to provide.

192. Defendant knew that Plaintiff and Class Members conferred a benefit upon it, which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

193. If Plaintiff and Class Members had known that Defendant had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

194. Due to Defendant's conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendant to be permitted to retain the benefit of its wrongful conduct.

195. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) an increase in spam calls, texts, and/or emails; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

196. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other

compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

197. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
Violations of Maryland's Consumer Protection Act and The Maryland Personal Information Act
(On Behalf of Plaintiff and the Class)

198. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein and bring this claim on behalf of themselves and the Class.

199. This cause of action is brought pursuant to the Maryland Consumer Protection Act, § 13-101, *et seq.* and the Maryland Personal Information Protection Act, § 14-3501, *et seq.*

200. The purpose of the Maryland Consumer Protection Act is "to set certain minimum statewide standards for the protection of consumers across the State [of] [Maryland]."

201. The Maryland Personal Information Protection Act was implemented to, among other things, "[t]o protect personal information from unauthorized access, use, modification, or disclosure...of an individual residing in the State [of] [Maryland]."

202. A violation of the Maryland Personal Information Protection Act "is an unfair or deceptive trade practice."

203. Defendant has violated the Maryland Personal Information Protection Act and, by extension, the Maryland Consumer Protection Act by engaging in the conduct alleged herein.

204. Independently, Defendant has violated the Maryland Consumer Protection Act by engaging in the unfair and deceptive practices alleged herein. Pursuant to HIPAA (42 U.S.C. §

1302d *et seq.*), the FTCA, and Maryland law, Defendant was required by law, but failed, to protect Plaintiff's and the Class's Private Information and maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Private Information. This constitutes a violation of Maryland's Consumer Protection Act.

205. The damages suffered by Plaintiff and Class Members were directly and proximately caused by the deceptive, misleading, and unfair practices of Defendant, as described above.

206. Plaintiff and Class Members seek declaratory judgment that Defendant's data security practices were not reasonable or adequate and caused the cyberattack under the Maryland CPA, as well as injunctive relief enjoining the above described wrongful acts and practices of Defendant and requiring Defendant to employ and maintain industry accepted standards for data management and security, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

207. Additionally, Plaintiff and Class Members make claims for actual damages, attorneys' fees, and costs.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class described above, seek the following relief:

a. An order certifying this action as a Class action, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendant to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Defendant to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: January 17, 2024

Respectfully submitted,

By: /s/ Courtney L. Weiner
Courtney L. Weiner (No. 19463)
LAW OFFICE OF COURTNEY WEINER PLLC
1629 K Street, NW, Suite 300
Washington, DC 20006
T: (202) 827-9980
cw@courtneyweinerlaw.com

Ken Grunfeld*
KOPELOWITZ OSTROW

FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
grunfeld@kolawyers.com

Attorneys for Plaintiff and the Putative Class

**pro hac vice forthcoming*

ClassAction.org
