UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF KENTUCKY

MELINDA FLEET, individually and on behalf of all similarly situated persons,	
Plaintiff,	Case No. 5:22-CV-109-BJB
v.	**JURY TRIAL DEMANDED**
SOUTHERN ORTHOPEDIC ASSOCIATES, P.S.C. D/B/A ORTHOPAEDIC INSTITUTE OF WESTERN KENTUCKY,	
Defendant.	

CLASS ACTION COMPLAINT

Plaintiff, Melinda Fleet ("Plaintiff"), individually, and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to her and upon information and belief as to all other matters, and by and through undersigned counsel, hereby brings this Class Action Complaint against Defendant, Southern Orthopedic Associates, P.S.C. d/b/a Orthopaedic Institute of Western Kentucky ("Defendant" or "SOA"), and alleges as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendant on behalf of herself and all others similarly situated for Defendant's failure to properly secure and safeguard Plaintiff's and Class members' personally identifiable information stored within Defendant's information network, including, without limitation, their names, Social Security numbers, driver's license numbers, passport numbers, financial account numbers and/or routing numbers, security code (CVV), payment card numbers, online account usernames and passwords, PIN or account logins, dates of birth (these types of information, *inter alia*, being hereafter referred to, collectively, as "personally identifiable information" or "PII")[1] and to properly secure and

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all

safeguard Plaintiff's and Class members' personal health information stored within Defendant's information network, including, without limitation, their medical billing/claims information, diagnosis, medical record number, Medicare/Medicaid identification, health information, health insurance information, and patient account number (this type of information, *inter alia*, being hereafter referred to, collectively, as "personal health information" or "PHI").[2]

2. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused Plaintiff and the over one hundred and six thousand (106,000) other similarly situated Class members in the massive and preventable ransomware attack that took place beginning on or around June 24, 2021 and continued through July 8, 2021, by which cybercriminals infiltrated Defendant's inadequately protected employee email accounts where highly sensitive personal and medical information was being kept unprotected (the "Data Breach" or "Breach").[3]

3. Unauthorized persons infiltrated Defendant's employee email accounts which contained patients' sensitive PII/PHI that included names, Social Security numbers, driver's license numbers, passport numbers, financial account numbers and/or routing numbers, security code (CVV), payment card numbers, online account usernames and passwords, PIN or account logins, dates of birth, their medical billing/claims information, diagnosis, medical record number, Medicare/Medicaid identification, health information, health insurance information, and patient account number.[4]

---

information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[2] PHI is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act (HIPAA). *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

[3] *See* https://www.prnewswire.com/news-releases/orthopaedic-institute-of-western-kentucky-provides-notice-of-data-privacy-event-301448413.html (last accessed June 14, 2022).

[4] *Id.*

4. This PII/PHI was compromised due to Defendant's negligent, grossly negligent, and/or reckless acts and omissions and the failure to protect PII/PHI of Plaintiff and Class members.

5. Due to Defendant's negligence, gross negligence, and/or recklessness and data security failures, cybercriminals obtained and now possess everything they need to commit personal and medical identity theft and wreak havoc on the financial and personal lives of hundreds of thousands of individuals for decades to come.

6. Defendant flagrantly disregarded Plaintiff's and Class members' privacy and property rights by intentionally, willfully and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiff's and other Class members' PII/PHI from unauthorized disclosure. Plaintiff's and Class members' PII/PHI was improperly handled, inadequately protected, readily able to be copied by thieves and not kept in accordance with basic security protocols. Defendant's obtaining of the information and sharing of same also represent a flagrant disregard of Plaintiff's and Class members' rights, both as to privacy and property.

7. The exposed PII/PHI of Plaintiff and Class members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII/PHI to criminals. Given Defendant's misconduct in allowing hackers to access such information in this instance, Plaintiff and Class members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

8. As a result of the Data Breach, Plaintiff and Class members have already suffered damages. For example, now that their PII/PHI been obtained by cybercriminals, Plaintiff and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives. Additionally, Plaintiff and Class members have already lost time and money responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

9. Plaintiff and the Class have also suffered and are entitled to damages for the lost benefit of the bargain with Defendant. Plaintiff and members of the Class paid Defendant

for its services including it protecting their PII/PHI. The lost benefit of the bargain is measured by the difference between the value of what Plaintiff and members of the Class should have received when they paid for Defendant's services and the value of what they actually received: services without adequate privacy safeguards. Plaintiff and members of the Class have been harmed in that they (1) paid more for privacy and confidentiality than they otherwise would have, and (2) paid for privacy protections they did not receive. In that respect, Plaintiff and Class members have not received the benefit of the bargain and have suffered an ascertainable loss.

10. Additionally, because of Defendant's conduct, Plaintiff and Class members have been harmed in that Defendant breached its common law fiduciary duty of confidentiality owed to Plaintiff and Class members.

11. Defendant acquired, collected, and stored Plaintiff's and Class members' PII/PHI in order to ensure efficient and quality healthcare to its patients.

12. The HIPAA Privacy Rule (45 CFR, Parts 160 and 164(A) and (E), among other sections, hereinafter "HIPAA") establishes national minimum standards for the protection of individuals' medical records and other personal health information. HIPAA, generally, applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, and sets minimum standards for Defendant's maintenance of Plaintiff's and Class members' personal and medical information. More specifically, HIPAA requires appropriate safeguards be maintained by healthcare providers such as Defendant to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. HIPAA also establishes a series of patients' rights over their health information, including rights to examine and obtain copies of their health records, and to request corrections thereto.

13. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative,

physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

14. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' PII/PHI, Defendant assumed legal and equitable duties to those individuals. These duties arise from HIPAA and other state/commonwealth and federal statutes and regulations as well as common law principles.

15. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class members' PII/PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII/PHI of Plaintiff and Class members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class members in the future. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

16. In addition to violating its purported commitment to its patients, explained *infra*, Defendant's failure to adequately secure Plaintiff's and Class members' sensitive data also breaches duties it owes Plaintiff and Class members under statutory and common law. Under HIPAA, healthcare providers have an affirmative duty to keep patients' PII/PHI private. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state/commonwealth statutes to safeguard Plaintiff's and Class members' data. Moreover, Defendant's promises of privacy and security induced Plaintiff and Class members to share their PII/PHI with Defendant. Plaintiff and Class members were entitled to, and did, rely on those promises. Because Defendant's promises foreseeably induced Plaintiff and Class members to act in reliance on those promises, Defendant had a duty to Plaintiff and Class members to fulfill those promises.

17. Defendant violated its duty to Plaintiff and Class members through its failure to protect against a foreseeable cyber-attack.

18. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's, treatment plans) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web.[5] Unsurprisingly, thus, the healthcare industry is at high risk and acutely affected by cyber-attacks.[6]

19. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.[7] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[8] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03% of overall health data breaches, according to cybersecurity firm Tenable.[9]

20. Health data breaches are particularly concerning because they can lead not only to the disclosure of sensitive data, but to substandard treatment and negative health outcomes.[10] The devastating consequences of network interruption for patients is what makes health systems so tempting a target for attacks in the first place. Cybercriminals view patient care facilities as being more likely to pay ransoms to restore access to their systems since extended

---

[5] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B4-healthcare-08-00133 (last accessed June 27, 2022) (citing Chernyshev, M., Zeadally, S. & Baig, Z. Healthcare Data Breaches: Implications for Digital Forensic Readiness. J Med Syst 43, 7 (2019).

[6] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4479128/. (last accessed June 27, 2022).

[7] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133. (last accessed June 27, 2022).

[8] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/. (last accessed June 27, 2022).

[9] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches. (last accessed June 27, 2022).

[10] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B8-healthcare-08-00133. (last accessed June 27, 2022).

downtime is intolerable.[11] Consequently, health data systems require enhanced security and should be breach-proof.[12]

21. Because hacking attacks using malware or ransomware represent a significant portion of all data breaches or unlawful disclosures, healthcare providers should be prepared for such attacks. Defendant knew or should have known that it was a prime target for such attacks. As such, Defendant's failure to protect against the attack was negligent and or reckless in violation of its legal duty to Plaintiff and Class members.

THE PARTIES

22. Defendant is a domestic for-profit Illinois corporation and has its principal place of business at 510 Lincoln Drive, Herrin, IL 62948. Defendant has named FBT LLC located at 400 West Market Street, 32nd Floor, Louisville, Kentucky 40202 as its agent for service of process.

23. Defendant's main clinic is located at 200 Clint Hill Boulevard, Paducah, Kentucky 42001.

24. Upon information and belief, Defendant's main clinic is the site where the Data Breach occurred.

25. Defendant is "the region's largest musculoskeletal service provider and offers treatment that rivals any found in larger cities."[13]

26. Defendant was founded in 2009. It "has nine skilled physicians on staff, along with therapists, athletic trainers, nurses, and medical assistants."[14]

27. Defendant is required to maintain the strictest privacy and confidentiality of Plaintiff and the Class members' medical records and other PHI and PII.

28. Plaintiff is a resident of Marshall County, Kentucky and is a former patient of Defendant.

---

[11] https://www.cpomagazine.com/cyber-security/rise-in-healthcare-data-breaches-driven-by-ransomware-attacks/. (last accessed July 28, 2021).

[12] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B8-healthcare-08-00133. (last accessed July 28, 2021).

[13] *See* https://oiwky.com/about-us/ (last accessed June 14, 2022).

[14] *Id.*

29. Plaintiff and the proposed Class members are current or former patients of Defendant. As part of its business operation, Defendant collects and maintains PHI and PII of its patients.

30. Plaintiff was a patient of Defendant, and, as a result, provided her PII/PHI to Defendant.

31. Plaintiff entered into an implied contract with Defendant for the adequate protection of her PII/PHI.

JURISDICTION AND VENUE

32. This Court has diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiff and many members of the class are citizens of states different from Defendant.

33. The Court has personal jurisdiction over Defendant because Defendant conducts substantial business in Kentucky and this District through its offices and affiliates.

34. Venue is proper in the Western District of Kentucky District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to this cause of action occurred in McCracken County, Kentucky. Therefore, venue is properly placed in the Paducah Division of the United States District Court for the Western District of Kentucky.

FACTUAL ALLEGATIONS

A. Defendant's inadequate data security exposed its current and former patients' sensitive PII/PHI

35. Beginning on or around June 24, 2021 an unknown third party gained access to Defendant's employee emails where highly sensitive patient data was contained unencrypted.

36. Plaintiff received a Notice Letter in late December 2021 providing her notice of the Data Breach. The Notice Letter was sent to her father's address. A sample Notice Letter is attached hereto as **Exhibit 1**.

37. The letter states: "[a]lthough we cannot confirm whether your personal information was actually accessed, viewed, or acquired without permission, we are providing you this notification…because such activity cannot be ruled out." *See* **Exhibit 1**.

38. The Notice Letter was sent to Plaintiff and the Class more than five months after the Data Breach began and includes the following:

> **What Happened?**
>
> On or about July 7, 2021, SOA became aware of suspicious activity relating to an employee email account. We immediately launched an investigation to determine what may have happened. Working together with an outside computer forensics specialist, we determined that an unauthorized individual accessed several employee email accounts between June 24, 2021 and July 8, 2021. Because we were unable to determine which email messages in the accounts may have been viewed by the unauthorized actor, we reviewed the entire contents of the affected email accounts to identify what personal information was accessible. This review was complete by October 21, 2021. Once we identified the individuals who may have been impacted, SOA worked to conform current mailing addresses for the impacted individuals and prepare an accurate written notice of this incident.
>
> **What Information Was Involved?**
>
> Although we cannot confirm whether your personal information was actually accessed, viewed, or acquired without permission, we are providing you this notification out of an abundance of caution, because such activity cannot be ruled out. The following types of your information were located in an email or attachment that may have been accessed or acquired by an unauthorized actor: name, date of birth, Social Security number, driver's license number, passport number, financial account number and/or routing number, security code (CVV), payment card number, online account username and password, PIN or account login, medical billing/claims information, diagnosis, medical record number, Medicare/Medicaid identification, health information, health insurance information, and patient account number.[15]
>
> **What We Are Doing.**
>
> Upon learning of this incident, we changed all employee email account passwords and took steps to secure the impacted accounts. We are currently

[15] *See, e.g.*, https://www.prnewswire.com/news-releases/orthopaedic-institute-of-western-kentucky-provides-notice-of-data-privacy-event-301448413.html.

> implementing additional technical safeguards as well as training and education for employees to prevent similar future incidents.

39. After receiving the notice letter, it is reasonable for recipients, including Plaintiff and Class members, to believe that the risk of future harm (including identity theft) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm. Defendant offered complimentary access to Experian IdentityWorks for twelve (12) months. *See* **Exhibit 1**.

40. Upon information and belief, the unauthorized third-party cybercriminals gained access to the PII/PHI with the intent of engaging in misuse of the PII/PHI, including marketing and selling Plaintiff's and Class members' PII/PHI.

41. In spite of the severity of the Data Breach, Defendant has done very little to protect Plaintiff and the Class. For example, in the notice, Defendant only provides twelve (12) months of identity theft and credit monitoring protection. This complimentary service is a token gesture that does little if anything to remedy the harm Defendant's misconduct caused. This does not and will not fully protect the patients from cybercriminals and is largely ineffective against protecting data after it has been stolen. Cybercriminals are fully aware of the well-publicized preventative measures taken by entities after data breaches such as that which happened here and will, therefore, oftentimes hold onto the stolen data and not use it until after the complimentary service is no longer active, and long after victim concerns and preventative steps have diminished.

42. In effect, Defendant is shirking its responsibility for the harm and increased risk of harm it has caused Plaintiff and members of the Class, including the distress and financial burdens the Data Breach has placed upon the shoulders of the Data Breach victims.

43. The notice letter fails to provide the consolation Plaintiff and Class members seek and certainly falls far short of eliminating the substantial risk of fraud and identity theft Plaintiff and the Class now face.

44. To make matters worse, Defendant's attackers actually gained access to Plaintiff's and Class members' PII/PHI.

45. It is unclear whether Defendant's email accounts required two-factor authorization. Many websites that do not host any personal information require such authorization. Any failure of Defendant to do so constitutes negligence.

46. Plaintiff's and Class members' information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII/PHI for targeted marketing without the approval of Plaintiff and/or Class members. Either way, unauthorized individuals can easily access the PII/PHI of Plaintiff and Class members.

B. The Cyber-attackers acted with actual malice

47. The cyber-attackers here acted with actual malice, with a criminal motive, and Plaintiff's data has been exposed as the result of a targeted attempt to obtain that data. Defendant's investigation into the attack confirmed its network was breached beginning on June 24, 2021 and continued through July 8, 2021.

48. The parts of the network accessed by the attackers contained patients' unsecured, protected health information.

C. Plaintiff has suffered actual misuse as a result of the Data Breach

49. Plaintiff has suffered actual misuse as a result of this Data Breach. As described more fully below, since the Data Breach, Plaintiff has received notifications, including from Credit Karma, suggesting fraudulent activity.

D. The type of data compromised here can be used for fraud and identity theft

50. The type of Plaintiff's data that was accessed and compromised here (including full name, Social Security number, addresses, and date of birth) can easily be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access due to their durability.

51. Social Security numbers and dates of birth together constitute high risk data.

52. Social Security numbers are the "gold standard" for identity theft.

53. Experience and common sense teach that Plaintiff faces a substantial risk of identity theft given that her Social Security number, address, and date of birth were accessed by a network intruder.

54. When a Social Security number is stolen it can forever be wielded to identify the victim and target him/her in fraudulent schemes and identity theft attacks.

E. The PII/PHI exposed by Defendant as a result of its inadequate data security is highly valuable on the black market

55. The information exposed by Defendant is a virtual goldmine for phishers, hackers, identity thieves and cybercriminals.

56. Stolen PII/PHI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

57. When malicious actors infiltrate companies and copy and exfiltrate the PII/PHI that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[16]

58. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[17]

---

[16] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last accessed June 27, 2022).

[17] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last accessed June 27, 2022).

59. The PII/PHI of consumers 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. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[18]. Criminals can also purchase access to entire company data breaches from $900 to $4,500[19].

60. Social Security numbers, for example, are among the worst kind of personal 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 is the case here, 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[20].

61. 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.

---

[18] *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 accessed June 27, 2022).

[19] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 28, 2021).

[20] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 27, 2022).

62. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The 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."[21]

63. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

64. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

65. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and Class members that their PII/PHI had been stolen. It took Defendant more than five months to notify Plaintiff of the compromise, despite Defendant's claim that it discovered the Data Breach before it ended.

66. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

67. Data breaches facilitate identity theft as hackers obtain consumers' PII/PHI and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

F. Defendant failed to comply with Federal Trade Commission requirements

68. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for

[21] 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 June 27, 2022).

businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[22]

69. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[23] Among other things, the guidelines note businesses should 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 security problems. 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.[24]

70. Additionally, the FTC recommends that companies 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.[25]

71. Highlighting the importance of protecting against phishing and other types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, 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 ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[26]

---

[22] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 27, 2022).

[23] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 27, 2022).

[24] *Id.*

[25] Federal Trade Commission, *Start With Security*, *supra footnote 17*.

[26] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*,

72. By negligently securing Plaintiff's and Class members' PII/PHI and allowing an unknown third-party cybercriminal to access Defendant's unencrypted, unprotected PII/PHI, Defendant failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data. Defendant's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

G. Defendant collected, stored, and maintained Plaintiff's and Class Members' PII/PHI

73. Defendant acquired, collected, and stored Plaintiff's and Class members' PII/PHI.

74. Indeed, personal health records can improve patient engagement, coordinate, and combine information from multiple healthcare providers, ensure availability of patient information online, reduce administrative costs and enhance provider-patient communication. Such benefits are a potent inducement to share even the most sensitive information with Defendant.

75. By obtaining, collecting, and storing Plaintiff's and Class members' PII/PHI, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII/PHI from unauthorized disclosure.

76. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their PII/PHI. Plaintiff and Class members relied on Defendant to keep their PII/PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

77. Defendant could have prevented this Data Breach by properly securing and encrypting Plaintiff's and Class members' PII/PHI.

---

https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited June 27, 2022).

78. Defendant's negligence in safeguarding Plaintiff's and Class members' PII/PHI is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

79. The healthcare industry has experienced a large number of high-profile cyber-attacks even in just the two-year period preceding the filing of this Complaint and cyber-attacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[27] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported in April 2021.[28]

80. For example, Universal Health Services experienced a cyber-attack on September 29, 2020. Universal Health Services suffered a four-week outage of its systems which caused as much as $67 million in recovery costs and lost revenue.[29] Due to the high-profile nature of the Universal Health Services breach, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack.

81. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class members' PII/PHI from being compromised.

H. Defendant had an obligation to protect PII/PHI under federal law and the applicable standard of care

82. As a direct and proximate result of Defendant's failure to properly safeguard and protect the PII/PHI of its patients, Plaintiff's and Class members' PII/PHI was stolen, compromised, and wrongfully disseminated without authorization.

---

[27] https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/ (last accessed June 27, 2022).

[28] https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/ (last accessed June 27, 2022).

[29] https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and (last accessed June 27, 2022).

83. Defendant had a duty to its patients to protect them from wrongful disclosures.

84. As a healthcare provider, Defendant is required to train and supervise its employees regarding the policies and procedures as well as the state and federal laws for safeguarding patient information.

85. Defendant is covered by HIPAA (45 C.F.R. § 160.102). As such, it 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.

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

87. 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.

88. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

89. "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.

90. 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;

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

d. Ensure compliance by their workforce.

91. 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), and 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).

92. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414 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."

93. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

94. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII/PHI of the Class.

95. Defendant owed a duty to Plaintiff and the Class to design, maintain, and test its computer systems and networks to ensure that the PII/PHI in its possession was adequately secured and protected.

96. Defendant owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the PII/PHI in its possession.

97. Defendant owed a duty to Plaintiff and the Class to implement processes that would detect a breach on its data security systems in a timely manner.

98. Defendant owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

99. Defendant owed a duty to Plaintiff and the Class to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII/PHI from theft because such an inadequacy would be a material fact in the decision to entrust PII/PHI with Defendant.

100. Defendant owed a duty of care to Plaintiff and the Class because they were foreseeable and probable victims of any inadequate data security practices.

101. Defendant owed a duty to Plaintiff and the Class to encrypt Plaintiff's and Class members' PII/PHI and monitor user behavior and activity in order to identity possible threats.

102. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH")[30]. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

104. 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).

105. Under HIPAA:

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

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.[31]

106. HIPAA and HITECH obligated Defendant to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

107. 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.

108. HIPAA further obligated Defendant to ensure that its workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

109. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on

[31] 45 C.F.R. § 160.103

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." *See* US Department of Health & Human Services, Security Rule Guidance Material.[32] 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." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[33]

110. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "[a] covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

(1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);

(2) the recipient of the PHI;

(3) whether the PHI was actually acquired or viewed; and

(4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed).[34]

[32] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
[33] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
[34] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304

111. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information.

112. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train its employees and staff so that all its staff and employees know their roles in facility security.

113. Defendant failed to provide proper notice to Plaintiff of the disclosure.

114. Defendant failed to conduct or improperly conducted the four-factor risk assessment following the unauthorized disclosure.

115. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, the criminal(s) and/or their customers now have Plaintiff's and the other Class members' compromised PHI and PII.

116. There is a robust international market for the purloined PHI and PII, specifically medical information. Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class members at an imminent, immediate, and continuing increased risk of identity theft, identity fraud[35] and medical fraud.

117. Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services, or goods. For example, as of 2010, more than 50 million people in the United States

[35]According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia,* credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

did not have health insurance according to the U.S. census. This, in turn, has led to a surge in medical identity theft as a means of fraudulently obtaining medical care.

118. Defendant flagrantly disregarded and/or violated Plaintiff's and Class members' privacy and property rights, and harmed them in the process, by not obtaining Plaintiff's and Class members' prior written consent to disclose their PII/PHI to any other person as required by laws, regulations, industry standards and/or internal company standards.

119. Defendant flagrantly disregarded and/or violated Plaintiff's and Class members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiff's and other Class members' PII/PHI to unauthorized persons.

I. Defendant was on notice of cyber-attack threats in the healthcare industry and of the inadequacy of its data security

120. Defendant was on notice that companies in the healthcare industry were targets for cyber-attacks.

121. Defendant was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyber-attack 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)."

122. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

123. Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyber-attacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.

124. As implied by the above quote from the AMA, stolen PII/PHI can be used to interrupt important medical services themselves. This is an imminent and certainly impending risk for Plaintiff and Class members.

125. Defendant was on notice that the federal government has been concerned about healthcare company data encryption. Defendant knew it kept protected health information on its servers and yet it appears Defendant did not encrypt this information.

126. The United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, the DHHS's Office of Human Rights' deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."

127. As a covered entity under HIPAA and other relevant statutes, Defendant should have known its systems were prone to ransomware and other types of cyberattacks and sought better protection for the PII/PHI accumulating in its system networks.

J. The value of PII and PHI

128. The data accessed in such an attack represents a major score for cybercriminals. This information is of great value to them and the data stolen in the Data Breach will be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class members and to profit off their misfortune.

129. Indeed, it is well known and the subject of many media reports that PII/PHI is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, Defendant maintained an insufficient and inadequate system to protect the PII/PHI of Plaintiff and Class members.

130. PII/PHI is a valuable commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground Internet websites.

131. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[36] For example, with the PII/PHI stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[37] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class members.

132. Indeed, it is well known and the subject of many media reports that PII/PHI is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, Defendant maintained an insufficient and inadequate system to protect the PII/PHI of Plaintiff and Class members.

133. PII/PHI is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.

134. For example, it is believed that certain PII/PHI compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class members for the rest of their lives. They will need to remain constantly vigilant for identity theft.

135. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone

---

[36] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[37] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/. (last accessed June 27, 2022).

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."

136. Identity thieves can use personal information, such as that of Plaintiff and Class members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

137. The ramifications of Defendant's failure to keep secure Plaintiff's and Class members' PII/PHI are long lasting and severe. Once PII/PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

138. The PII/PHI of Plaintiff and Class members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII/PHI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

139. In this context, at all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Plaintiff's and Class members' PII/PHI, including Social Security numbers and/or dates of birth, 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.

140. As a result of the Data Breach, the PII/PHI of Plaintiff and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class members, or likely to be suffered thereby as a direct result of Defendant's Data Breach, include:

a. unauthorized use of their PII/PHI;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII/PHI;

e. Improper disclosure of their PII/PHI;

f. loss of privacy, and embarrassment;

g. trespass and damage their personal property, including PII/PHI;

h. the imminent and certainly impending risk of having their confidential medical information used against them by spam callers and/or hackers targeting them with phishing schemes to defraud them;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

j. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII/PHI being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet black market; and

k. damages to and diminution in value of their PII/PHI entrusted to Defendant for the sole purpose of obtaining medical services from Defendant; and the loss of Plaintiff's and Class members' privacy.

141. The harm to Plaintiff and Class members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most

difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[38]

142. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[39]

143. If cybercriminals manage to access financial information, health insurance information, and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may expose the Plaintiff and Class members.

144. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[40] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[41]

145. The injuries to the Plaintiff and Class members were directly and proximately cause by Defendant's failure to implement or maintain adequate data security measures for this PII/PHI.

146. The Data Breach was the inevitable result of Defendant's inadequate approach to data security and the protection of the PII/PHI that it collected during the course of business

---

[38] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/. (last accessed June 27, 2022).

[39] *Id*.

[40] See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[41] Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/. (last accessed June 27, 2022).

and, as such, Defendant could have prevented this Data Breach. It had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

147. Had Defendant remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the Data Breach and, ultimately, the theft of its patients' PII/PHI.

148. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Class members are incurring and will continue to incur such damages in addition to any actual fraudulent usage of their PII/PHI.

149. 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 PII/PHI of Plaintiff and Class members.

150. This was a financially motivated Data Breach, as apparent from the ransom money sought by the cybercriminals, who will continue to seek to profit off of the sale of Plaintiff's and the Class members' PII/PHI on the dark web. The PII/PHI exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein.

151. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[42]

152. Data breaches are preventable.[43] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[44] She added that "[o]rganizations that collect, use, store, and

---

[42] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info. (last accessed June 27, 2022).

[43] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[44] *Id.* at 17.

share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[45]

153. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[46]

154. Defendant required Plaintiff and Class members to surrender their PII/PHI – including but not limited to their names, addresses, Social Security numbers, and medical information – and was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such PII/PHI.

155. Many failures laid the groundwork for the success ("success" from the cybercriminals' viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security protections, procedures, and protocols necessary to safeguard Plaintiff's and Class members' PII/PHI. Yet it did not do so.

156. Defendant knew of the importance of safeguarding Plaintiff's and Class members' PII/PHI and of the foreseeable consequences that would occur if Plaintiff's and Class members' PII/PHI was stolen, including the significant costs that would be placed on Plaintiff and Class members as a result of a breach of this magnitude.

157. Defendant is a sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff, Class members, and all of its former and current patients. Its failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

158. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class members' PII/PHI was a known risk to Defendant, and thus Defendant

---

45 *Id.* at 28.
46 *Id.*

was on notice that failing to take necessary steps to secure Plaintiff's and Class members' PII/PHI from those risks left that information in a dangerous condition.

159. Defendant disregarded the rights of Plaintiff and Class members by, inter alia, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class members' PII/PHI; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

160. The actual and adverse effects to Plaintiff and Class members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's wrongful actions and/or inaction, *infra*, and the resulting Data Breach require Plaintiff and Class members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class members have suffered, and will continue to suffer, such damages for the foreseeable future.

K. The U.S. Department of Health and Human Services Breach Report

157. A breach report regarding the Data Breach filed by Defendant with the Secretary of the U.S. Department of Health and Human Services states that 106,910 individuals were impacted by the Data Breach (the "Breach Report"). The Breach Report also characterizes the Healthcare Data Breach as a "hacking/IT incident" and further indicates that the breached information was accessed through email.[47]

[47] *See*

158. The U.S. Department of Health and Human Services designated Defendant as a "covered entity."[48]

159. The Breach Report was filed in accordance with 45 CFR § 164.408(a).

160. Plaintiff's and Class members' medical information is Protected Health Information as defined by 45 CFR § 160.103.

161. Pursuant to 45 CFR § 164.408(a), breach reports are filed with the Secretary of the U.S. Department of Health and Human Services "following the discovery of a breach of unsecured protected health information."

162. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

163. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

164. Plaintiff's and Class members' medical information is unsecured Protected Health Information as defined by 45 CFR § 164.402.

165. Plaintiff's and Class members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

---

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=8FC847D673798DF324DAFF0EA5F0D883 (last accessed June 27, 2022).

[48] *Id.*

166. Pursuant to the notice letter and Breach Report, Defendant reasonably believes Plaintiff's and Class members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

167. Plaintiff's and Class members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized person or persons.

168. Pursuant to the notice letter and Breach Report, Defendant reasonably believes Plaintiff's and Class members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized person or persons.

169. Plaintiff's and Class members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized person or persons.

170. Plaintiff's and Class members' unsecured protected health information was viewed by unauthorized person or persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

171. Pursuant to the notice letter and Breach Report, Defendant reasonably believes Plaintiff's and Class members' unsecured protected health information was viewed by

unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

172. It is reasonable to infer that Plaintiff's and Class members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized person or persons.

173. It should be presumed that unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized person or persons.

174. After receiving notice that they were victims of a breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class members in this case, to believe that present and continuing harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of present and continuing harm.

175. Based upon Defendant's post-disclosure ongoing duty, it is reasonable to assume that Defendant believes that its patients are at risk for present and continuing identity theft as warnings of possible identity theft were included in the Breach Notice.

L. Plaintiff's experience

176. Plaintiff is a former patient of Defendant's.

177. In or around December 2021, Plaintiff received a notice letter from Defendant informing her of the Data Breach.

178. After receiving notification of the Data Breach, Plaintiff began receiving notifications of potential fraudulent activity from her bank as well as from Credit Karma.

179. As a direct and traceable result of the Data Breach, Plaintiff has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This is time that has been lost forever and cannot be recaptured.

180. Plaintiff is very careful about sharing her PII/PHI. She has never knowingly transmitted unencrypted PII/PHI over the internet or any other unsecured source.

181. Plaintiff stores all documents containing her PHI/PII in a safe and secure location.

182. Plaintiff has suffered actual, concrete injury in the form of damages to, and diminution in, the value of her PII/PHI – forms of intangible property that Plaintiff entrusted to Defendant for the purpose of her medical care. Her PHI/PII was compromised in, and has been diminished as a result of, the Data Breach.

183. Plaintiff has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress, anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

184. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII/PHI resulting from the compromise of her PII/PHI, especially her Social Security number, in combination with her full name, along with her sensitive medical diagnoses, which PII/PHI is now in the hands

of cybercriminals and other unauthorized third parties.

185. Knowing that thieves stole her PII/PHI, including her Social Security number and medical diagnoses, and knowing that her PHI/PII will be sold on the dark web has caused Plaintiff great anxiety.

186. Additionally, Plaintiff has never knowingly transmitted unencrypted PII/PHI over the internet or any other unsecured source. She deletes any and all electronic documents containing her PHI/PII and destroys any documents that may contain any of her PHI/PII, or that may contain any information that could otherwise be used to compromise her PHI/PII.

187. Plaintiff has a continuing interest in ensuring that her PHI/PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

188. As a direct and traceable result of the Data Breach, Plaintiff will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of her life to protect her exposed PII/PHI.

M. Plaintiff and the Class members suffered damages

189. The ramifications of Defendant's failure to keep current and former patients' PII/PHI secure are long lasting and severe. Once PII/PHI is stolen, fraudulent use of that information and damage to victims may continue for years.[49]

190. The PII/PHI belonging to Plaintiff and Class members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or

[49] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed June 27, 2022).

Class members' consent to disclose such PII/PHI to any other person as required by applicable law and industry standards.

191. Defendant required Plaintiff and Class members to provide their PII, including full names and Social Security numbers in order to obtain medical care from Defendant. Implied in these exchanges was a promise by Defendant to ensure that the PII/PHI of Plaintiff and Class members in its possession was only used to provide agreed-upon medical services from Defendant.

192. Plaintiff and Class members, therefore, did not receive the benefit of the bargain with Defendant, because providing their PII/PHI to Defendant was in exchange for Defendant's implied agreement to secure it and keep it safe.

193. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff's and Class members' PII/PHI from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

194. Defendant had the resources necessary to prevent the Data Breach, but neglected to implement adequate data security measures, despite its obligations to protect current and former patients' PII/PHI.

195. Had Defendant remedied the deficiencies in its data security training and protocols and adopted security measures recommended by experts in the field, it would have prevented the intrusion leading to the theft of PII/PHI.

196. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

197. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[50]

198. As a direct result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII/PHI;

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

[50] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed June 27, 2022).

d. The continued risk to their PII/PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII/PHI in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

199. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring that their PII/PHI is secure, remains secure, and is not subject to further misappropriation and theft.

200. To date, other than providing a woefully inadequate twelve (12) months of credit monitoring and identity protection services, Defendant does not appear to be taking any measures to assist Plaintiff and Class members other than simply telling them to review their financial records and credit reports on a regular basis.

201. This type of recommendation, however, does not require Defendant to expend any effort to protect Plaintiff's and Class members' PII/PHI.

202. Defendant's failure to adequately protect Plaintiff's and Class members' PII has resulted in Plaintiff and Class members having to undertake tasks requiring extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sits by and does nothing to assist those affected by the Data Breach. Instead, as Defendant's notice letter indicates, it is putting the burden on Plaintiff and Class members to discover possible fraudulent activity and identity theft.

203. Defendant's offer of twelve (12) months of identity monitoring and identity protection services to Plaintiff and Class members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII/PHI is acquired and when it is used. Furthermore, identity theft monitoring services only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII/PHI) – they do not prevent identity theft.[51] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection. Although their PII/PHI was improperly exposed beginning in June 2021, affected current and former patients were not notified of the Data Breach until more than five months later, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendant's delay in detecting and notifying current and former patients of the Data Breach, the risk of fraud for Plaintiff and Class members has been driven even higher.

N. Defendant also failed to adequately protect its patients' Payment Data[52]

204. It is well known that sensitive Payment Data is valuable and frequently targeted by hackers. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses…"[53]

---

[51] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited June 27, 2022).

[52] "Payment Data" as used herein includes, but is not limited to, financial account numbers and/or routing numbers, security code (CVV), and payment card numbers.

[53] Dennis Green & Mary Hanbury, "If you bought anything from these 11 companies in the last year, your data may have been stolen," BUSINESS INSIDER (Aug. 15, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

205. Despite the known risk of a data breach and the widespread publicity and industry alerts regarding the other notable data breaches, Defendant failed to take reasonable steps to adequately protect its computer systems from being breached, and then failed to detect the Data Breach for several months.

206. Defendant is, and at all relevant times has been, aware that the Payment Data it maintains as a result of payments made by its patients is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases.

207. Financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure that consumers' (or here, patients') valuable data is protected.

208. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires entities such as Defendant to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

209. The twelve requirements of the PCI DSS are:

a. Install and maintain a firewall configuration to protect cardholder data;
b. Do not use vendor-supplied defaults for system passwords and other security parameters;
c. Protect stored cardholder data;
d. Encrypt transmission of cardholder data across open, public networks;
e. Protect all systems against malware and regularly update anti-virus software or programs;
f. Develop and maintain secure systems and applications;

g. Restrict access to cardholder data by business need to know;
h. Identify and authenticate access to system components;
i. Restrict physical access to cardholder data;
j. Track and monitor all access to network resources and cardholder data;
k. Regularly test security systems and processes; and
l. Maintain a policy that addresses information security for all personnel.[54]

210. Furthermore, PCI DSS sets forth detailed and comprehensive requirements that must be followed to meet each of the twelve mandates.

211. Defendant was always fully aware of its data protection obligations in light of its participation in its payment card processing system's collection and transmission of thousands of sets of Payment Data.

212. Because Defendant accepted payment cards containing sensitive financial information, it knew that its patients were entitled to and did in fact rely on it to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements. Nevertheless, Defendant did not adhere to the PCI DSS requirements.

213. Additionally, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45. *See, e.g.*, *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 245-47 (3d Cir. 2015); *In re BJ's Wholesale Club, LLC*, 140 F.T.C. 465 (2005).

214. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal

[54] Payment Card International (PCI) Data Security Standard, "Requirements and Security Assessment Procedures, Version 3.2.1," (May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1574069601944.

customer 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 for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying 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.

215. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[55]

216. The FTC has issued orders against businesses that failed to employ reasonable measures to secure Payment Data. These orders provide further guidance to businesses in regard to their data security obligations.

217. Defendant knew or should have known of the need to have adequate, updated data security systems in place.

218. Despite this, Defendant failed to update and maintain its data security systems in a meaningful way so as to prevent data breaches. Defendant's security flaws run afoul of industry best practices and standards. More specifically, the security practices in place at Defendant are in stark contrast and directly conflict with the PCI DSS core security standards.

219. Had Defendant maintained its information technology systems ("IT systems"),

---

[55] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 27, 2022).

adequately protected them, and had adequate security safeguards in place, it could have prevented the Data Breach.

220. As a result of industry warnings, awareness of industry best practices, the PCI DSS, and numerous well-documented data breaches, Defendant was alerted to the risk associated with failing to ensure that its IT systems were adequately secured.

221. Defendant, at all times relevant to this action, had a duty to Plaintiff and members of the Class to: (a) properly secure Payment Data submitted to it or collected by it; (b) encrypt Payment Data using industry standard methods; (c) use available technology to defend its system from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiff and the Class that would naturally result from Payment Data theft; and (e) promptly notify patients when Defendant became aware of the potential that its patients' Payment Data would be compromised.

222. Defendant failed in all the aforementioned obligations. Instead, Defendant permitted patients' Payment Data to be compromised by failing to take reasonable steps against an obvious threat.

223. In addition, leading up to the Data Breach, and during the Breach itself and the investigation that followed, Defendant failed to follow the guidelines set forth by the FTC.

224. Industry experts are clear that a data breach is indicative of data security failures. Indeed, Julie Conroy—research director at the research and advisory firm Aite Group—has identified that, "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[56]

[56] Lisa Baertlein, "Chipotle Says Hackers Hit Most Restaurants in Data Breach," REUTERS (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY.

225. Clearly, had Defendant utilized adequate data security and data breach precautions and response protocols, the window of the Data Breach would have been significantly mitigated, and the level of impact could have been reduced (or not permitted to happen in the first place).

226. Due to Defendant's inadequate security and failure to remediate the problem in a timely manner, Plaintiff and Class members' Payment Data is now in the hands of cybercriminals who can quickly turn a profit by posting the Payment Data on the dark web.

227. As a result of the events detailed herein, Plaintiff and members of the Class suffered actual, palpable fraud and losses resulting from the Data Breach, including lost control over the value of Payment Data, for which there is a well-established and quantifiable national and international market; loss of time and money expended in responding to the Data Breach and attempting to mitigate the harms of the Data Breach; loss of time and money resolving fraudulent charges and obtaining new debit and/or credit cards; loss of time obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Payment Data.

228. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges occur and are discovered.

229. For example, the Payment Data stolen from Defendant can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less-secure websites. To date, Defendant is not taking any real measures to assist affected patients other than providing a woefully inadequate twelve (12) months of free credit monitoring.

230. Defendant has only slowly provided information about the Data Breach at its own pace over the course of five months, leaving victims of the Data Breach in the dark and

vulnerable to continued fraud.

231. Defendant's failure to adequately protect its patients' Payment Data resulted in patients having to expend extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of their own money—while Defendant did little to assist those affected by the Data Breach, and withholding important details about the Data Breach as it conducts its investigation.

CLASS ACTION ALLEGATIONS

232. Plaintiff brings this action individually and on behalf of all members of the following classes of similarly situated persons (collectively, the "Class" or "Class members") under Rule 23 of the Federal Rules of Civil Procedure:

Nationwide Class

All persons residing in the United States who are current or former patients of Defendant and had their PII/PHI compromised by an unknown third-party cybercriminal as a result of the Data Breach that occurred between June 24, 2021 and July 8, 2021.

Kentucky Subclass

All persons residing in the Commonwealth of Kentucky who are current or former patients of Defendant and had their PII/PHI compromised by an unknown third-party cybercriminal as a result of the Data Breach that occurred between June 24, 2021 and July 8, 2021.

Excluded from the proposed Class are any officer or director of Defendant; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

233. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

234. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class members and predominate over questions affecting only individual Class members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's inadequate data security measures were a cause of the Data Breach;

c. Whether Defendant owed a legal duty to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their PII/PHI;

d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff and the Class members to exercise due care in collecting, storing, and safeguarding their PII/PHI;

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices for Plaintiff's and Class members' PII/PHI in violation Section 5 of the FTC Act;

g. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

h. Whether Plaintiff and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief

and restitution.

235. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

236. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. All Class members were subject to the Data Breach and had their PII/PHI accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class members in the same manner.

237. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class members she seeks to represent; she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

238. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create

a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION
Negligence
(On behalf of Plaintiff and the Nationwide Class)

239. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

240. As their healthcare provider, Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class members' PII/PHI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiff's and Class members' PII/PHI in Defendant's possession was adequately secured and protected.

241. Defendant owed a duty of care to Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that its protocols, systems, and networks adequately protected the PII/PHI of its current and former patients.

242. Defendant owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII/PHI of its current and former patients on an unsecured system, and the critical importance of adequately securing such information.

243. Plaintiff and Class members entrusted Defendant with their PII/PHI with the understanding that Defendant would safeguard it, that Defendant would not store it longer than

necessary, and that Defendant was in a position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach.

244. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PII/PHI. Defendant's misconduct included failing to implement the necessary systems, policies, employee training and procedures necessary to prevent the Data Breach.

245. Defendant failed to provide adequate supervision and oversight of the PII with which it was, and is, entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' PII/PHI, misuse the PII/PHI and intentionally disclose it to others without consent.

246. Defendant knew, or should have known, of the risks inherent in collecting and storing PII/PHI and the importance of adequate security. Defendant knew about – or should have been aware of – numerous, well-publicized data breaches affecting businesses and healthcare providers in the United States.

247. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PII/PHI of Plaintiff and Class members.

248. Plaintiff's injuries and damages, as described below, are a reasonably certain consequence of Defendant's breach of its duties.

249. Because Defendant knew that a breach of its systems would damage thousands of current and former patients whose PII/PHI was inexplicably contained unencrypted, Defendant had a duty to adequately protect its data systems and the PII/PHI contained therein.

250. Defendant had a special relationship with patients, including with Plaintiff and

Class members, by virtue of their being current and former patients of Defendant. Plaintiff and Class members reasonably believed that Defendant would take adequate security precautions to protect their PII/PHI. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class members' PII/PHI.

251. Implied in these exchanges was a promise by Defendant to ensure that the PII/PHI of Plaintiff and Class members in its possession was only used to provide the agreed-upon medical services from Defendant.

252. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness with regard to providing the agreed-upon medical services to Plaintiff and Class members and protecting Plaintiff's and Class members' PII/PHI.

253. Plaintiff and Class members did not receive the benefit of the bargain with Defendant, because providing their PII/PHI was in exchange for Defendant's implied agreement to secure and keep it safe.

254. Defendant also had independent duties under state and federal laws that required it to reasonably safeguard Plaintiff's and Class members' PII/PHI and promptly notify them about the Data Breach.

255. Through Defendant's acts and omissions, including Defendant's failure to provide adequate security and its failure to protect Plaintiff's and Class members' PII/PHI from being foreseeably accessed, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII/PHI of Plaintiff and Class members during the time it was within Defendant's possession or control.

256. The law further imposes an affirmative duty on Defendant to timely disclose

the unauthorized access and theft of the PII/PHI to Plaintiff and the Class members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII/PHI. Defendant failed to do so, only disclosing the Data Breach five (5) months after it began.

257. In engaging in the negligent acts and omissions as alleged herein, which permitted an unknown third party to access Defendant's system containing the PII/PHI at issue, Defendant failed to meet the data security standards set forth under Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures, which Defendant has failed to do as discussed herein.

258. Upon information and belief, Defendant improperly and inadequately safeguarded Plaintiff's and Class members' PII/PHI in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendant's failure to take proper security measures to protect Plaintiff's and Class members' sensitive PII/PHI, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of the PII/PHI.

259. Upon information and belief, neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their PI/PHI as described in this Complaint.

260. As a direct and proximate cause of Defendant's actions and inactions, including but not limited to its failure to properly encrypt its systems and otherwise implement and maintain reasonable security procedures and practices, Plaintiff and Class members have suffered and/or will suffer concrete injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII/PHI is used; (ii) the

publication and/or theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protection; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI of current and former patients in its continued possession; and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of Plaintiff and the Nationwide Class)

261. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

262. When Plaintiff and Class members provided their PII/PHI to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

263. Defendant required Plaintiff and the Class to provide their PII/PHI in order to receive medical services from Defendant.

264. Implied in these exchanges was a promise by Defendant to ensure the PII/PHI of Plaintiff and Class members in its possession was only used to provide medical services from Defendant, and that Defendant would take adequate measures to protect Plaintiff's and Class members' PII/PHI.

265. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiff's and Class members' PII/PHI to be accessed in the Data Breach.

266. Indeed, implicit in the agreement between Defendant and its patients was the obligation that both parties would maintain information confidentially and securely.

267. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Class members would provide their PII/PHI in exchange for medical services provided by Defendant. These agreements were made by Plaintiff and Class members being patients of Defendant.

268. It is clear by these exchanges that the parties intended to enter into an agreement and mutual assent occurred. Plaintiff and Class members would not have disclosed their PII/PHI to Defendant but for the prospect of Defendant's promise of medical services. Conversely, Defendant presumably would not have taken Plaintiff's and Class members' PII/PHI if it did not intend to provide Plaintiff and Class members medical services.

269. Through their course of conduct, Defendant, Plaintiff and Class members entered into implied contracts for the provision of medical care and treatment, as well as implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class members' PII/PHI.

270. Defendant solicited and invited Class members to provide their PII/PHI as part

of Defendant's regular business practices, in exchange for medical services and the protection of Plaintiff's and Class members' PII/PHI. Plaintiff and Class members accepted Defendant's offers and provided their PII/PHI to Defendant.

271. Through its conduct, Defendant manifested its assent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiff's and Class members' PII/PHI.

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

273. Plaintiff and Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

274. There was a meeting of the minds between the Parties as to this implied contract for data security. Plaintiff and Class members understood and believed they were providing their PII/PHI under a promise to keep that information safe and confidential, and Defendant manifested its assent to do so by its conduct and its express representations about data privacy.

275. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their PII/PHI associated with obtaining healthcare private. To customers such as Plaintiff and Class members, healthcare that does not adhere to industry standard data security protocols to protect PII/PHI is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

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

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

277. Plaintiff and Class members fully and adequately performed their obligations under the implied contracts with Defendant.

278. Defendant breached its implied contracts with Plaintiff and Class members by failing to safeguard and protect their PII/PHI.

279. Defendant's failure to implement adequate measures to protect the PII/PHI of Plaintiff and Class members violated the purpose of the agreement between the parties: medical services provided by Defendant to Plaintiff and Class members.

280. Defendant was on notice that its systems could be vulnerable to unauthorized access yet failed to invest in proper safeguarding of Plaintiff's and Class members' PII/PHI.

281. As a direct and proximate result of Defendant's breaches of the implied contracts, Class members sustained damages as alleged herein.

282. Plaintiff and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

283. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

284. Defendant offered medical services to the current or former patients, including Plaintiff and Class members, in exchange for receiving their PII/PHI.

THIRD CAUSE OF ACTION
Breach of Fiduciary Duty

(On behalf of Plaintiff and the Nationwide Class)

285. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

286. Kentucky has long recognized that the relationship between a physician and patient is a fiduciary relationship. *Emberton v. GMRI, Inc.*, 299 S.W.3d 565, 574 (Ky. 2009) (citing *Adams v. Ison*, 249 S.W.2d 791, 793 (Ky. Ct. App. 1952)).

287. In light of their special relationship as a medical provider to Plaintiff and Class members, Defendant became the guardian of Plaintiff's and Class members' PII/PHI. Defendant became a fiduciary, created by its undertaking and guardianship of its current and former patients' PII/PHI, to act primarily for the benefit of those patients, including Plaintiff and Class members. This duty included the obligation to safeguard Plaintiff's and Class members' PII/PHI and to timely detect and notify them in the event of a data breach.

288. In order to provide Plaintiff and Class members medical services, Defendant required that Plaintiff and Class members provide their PII/PHI.

289. Defendant knowingly undertook the responsibility and duties related to the possession of Plaintiff's and Class members' PII/PHI for the benefit of Plaintiff and Class members in order to provide Plaintiff and Class members medical services.

290. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its relationship with them. Defendant breached its fiduciary duties owed to Plaintiff and Class members by failing to properly encrypt and otherwise protect Plaintiff's and Class members' PII/PHI. Defendant further breached its fiduciary duties owed to Plaintiff and Class members by failing to timely detect the Data Breach and notify and/or warn Plaintiff and Class members of the Data Breach.

291. As a direct and proximate result of Defendant's breaches of its fiduciary duties,

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

292. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FOURTH CAUSE OF ACTION
Violation of the Kentucky Consumer Protection Act
KRS 367.110, et seq.
(On Behalf of Plaintiff and the Kentucky Subclass)

293. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

294. The Kentucky Consumer Protection Act prohibits any "unfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce." KRS 367.170.

295. Defendant is a "person" as defined by KRS 367.110.

296. Defendant engaged in the complained-of conduct in connection with "trade" and "commerce" with regard to "services" as defined by KRS 367.110. Defendant advertised, offered, or sold services relating to the medical treatment of Plaintiff and Kentucky Subclass members.

297. Defendant engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with trade and commerce, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kentucky Subclass members' PII/PHI, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff' and Kentucky

Subclass members' PII, which was a direct and proximate cause of the Data Breach;

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

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Kentucky Subclass members' PII/PHI; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kentucky Subclass members' PII/PHI.

298. Defendant intended to mislead Plaintiff and Kentucky Subclass members and induce them to rely on its misrepresentations and omissions in order to provide medical services to Plaintiff and Kentucky Subclass members.

299. Defendant's representations and omissions, made at the time of the relevant transactions, were material because they were likely to deceive reasonable consumers, including Plaintiff and Kentucky Subclass members, about the adequacy of Defendant's computer and data security.

300. Had Defendant disclosed to Plaintiff and Kentucky Subclass members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security

measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Kentucky Subclass members' PII/PHI as part of the relationship between Defendant and Plaintiff and Kentucky Subclass members without advising Plaintiff and Kentucky Subclass members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Kentucky Subclass members' PII/PHI. Accordingly, Plaintiff and the Kentucky Subclass members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

301. Defendant had a duty to disclose these facts due to the circumstances of this case and the sensitivity and extensivity of the PII/PHI in its possession. In addition, such a duty is implied by law due to the nature of the relationship between patients—including Plaintiff and the Kentucky Subclass—and Defendant, because patients are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendant. Defendant's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems while purposefully withholding material facts from Plaintiff and the Kentucky Subclass that contradicted these representations.

302. Defendant acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiff and Kentucky

Subclass members' rights. Defendant was on notice that its security and privacy protections were inadequate. An award of punitive damages would serve to punish Defendant for its wrongdoing and warn or deter others from engaging in similar conduct.

303. As a direct and proximate result of Defendant's deceptive acts or practices, Plaintiff and Kentucky Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have sought medical services from Defendant but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII/PHI; and an increased, imminent risk of fraud and identity theft.

304. Defendant's violations present a continuing risk to Plaintiff and Kentucky Subclass members as well as to the general public.

305. Plaintiff and Kentucky Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, and attorneys' fees and costs.

FIFTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

306. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

307. Plaintiff and the Class had a legitimate expectation of privacy to their PII/PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

308. Defendant owed a duty to its patients, including Plaintiff and the Class, to keep their PII/PHI contained as a part thereof, confidential.

309. Defendant failed to protect and released to unknown and unauthorized third parties the PII/PHI of Plaintiff and the Class.

310. Defendant allowed unauthorized and unknown third parties access to and examination of the PII/PHI of Plaintiff and the Class, by way of Defendant's failure to protect the PII/PHI.

311. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII/PHI of Plaintiff and the Class is highly offensive to a reasonable person.

312. The intrusion was into a place or thing which was private and is entitled to be private. Plaintiff and the Class disclosed their PII/PHI to Defendant as a requirement to receive medical services from Defendant, but privately with an intention that the PII/PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

313. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Class's interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

314. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were inadequate and insufficient.

315. Defendant acted with reckless disregard for Plaintiff's and Class members' privacy when it allowed improper access to its systems containing Plaintiff's and Class members' PII/PHI.

316. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class members' data.

317. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

318. As a proximate result of the above acts and omissions of Defendant, the PII/PHI of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

319. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class in that the PII/PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of herself and all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the proposed Class as requested herein;

b. Appointing Plaintiff as Class Representative and the undersigned counsel as Class Counsel;

c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

d. Granting injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII/PHI of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;

iv. requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII/PHI of Plaintiff's and Class members' PII/PHI;

v. prohibiting Defendant from maintaining Plaintiff's and Class members' PII/PHI on a cloud-based database;

vi. requiring Defendant to engage independent third-party

security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with

handling PII/PHI, as well as protecting the PII/PHI of Plaintiff and Class members;

xii. requiring Defendant to conduct internal training and education routinely and continually and, on an annual basis, inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII/PHI;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PII/PHI to third parties, as well as the steps affected individuals must take to protect

themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xviii. requiring Defendant to design, maintain, and test its computer systems to ensure that PII/PHI in its possession is adequately secured and protected;

xix. requiring Defendant to detect and disclose any future data breaches in a timely and accurate manner;

xx. requiring Defendant to implement multi-factor authentication requirements, if not already implemented;

xxi. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxii. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class

members.

e. Awarding Plaintiff and Class members damages;

f. Awarding Plaintiff and Class members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the proposed Class, hereby demands a trial by jury as to all matters so triable.

Date: August 16, 2022

Respectfully Submitted,

/s/ Jeremy T. Pruitt

Jeremy T. Pruitt (98146)
PRUITT LAW, PLLC
705 Main Street
Murray, KY 42071
270-917-1001 ext. 1
jpruitt@pruittlawky.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
Email: Wbf@federmanlaw.com

Lori G. Feldman*
GEORGE GESTEN MCDONALD, PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Phone: (917) 983-9321
Fax: (888) 421-4173
Email: LFeldman@4-Justice.com
E-Service: eService@4-Justice.com

David J. George*
Brittany L. Brown*
GEORGE GESTEN MCDONALD, PLLC
9897 Lake Worth Road, Suite #302 Lake Worth, FL 33467
Phone: (561) 232-6002
Fax: (888) 421-4173
Email: DGeorge@4-Justice.com
BBrown@4-Justice.com

**pro hac vice* applications forthcoming