UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

CASE NO.: 8:23-cv-01864-KKM-UAM

ANGELICA DIPIERRO, et al, *on behalf of themselves and all others similarly situated*,

Plaintiffs,

v.

Florida Health Sciences Center, Inc. d/b/a Tampa General Hospital, a Florida corporation,

Defendant.

AMENDED CLASS ACTION COMPLAINT

Plaintiffs, Angelica DiPierro, Amber Fields, Stacey Graham, Deborah Ivey, Edward James, Sr., Keon Critchlow, and Aubrey Rassel ("Plaintiffs"), file this Amended Class Action Complaint ("Complaint") against Defendant, Florida Health Sciences Center, Inc. d/b/a Tampa General Hospital ("Defendant" or "TGH"), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions, and upon information and belief and their counsels' investigation as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs seek monetary damages and injunctive and declaratory relief arising from Defendant's failure to safeguard the Personally Identifiable Information[1] ("PII") and Protected

[1] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R.

Health Information ("PHI") (collectively "Private Information") of its patients, which resulted in unauthorized access to its information systems on or around May 12, 2023, through May 30, 2023, and the compromised and unauthorized disclosure of that Private Information, causing widespread injury and damages to Plaintiffs and the proposed Class (defined below) members.

2. Defendant, a Tampa, Florida-headquartered company, is a private not-for-profit hospital serving over 4 million people in West Central Florida.

3. As alleged in detail herein, on or around May 31, 2023, Defendant detected unusual activity in its computer systems and ultimately determined that an unauthorized third party accessed its computer systems and obtained certain files from those systems between May 12, 2023 and May 30, 2023 ("Data Breach").[2]

4. As a result of the Data Breach, which Defendant failed to prevent, the Private Information of Defendant's patients, including Plaintiffs and the proposed Class members, were stolen, including their names, addresses, phone numbers, dates of birth, Social Security numbers, health insurance information, medical record numbers, patient account numbers, dates of service and/or limited treatment information used by Defendant for its business operations.[3]

5. Defendant's investigation concluded that the Private Information compromised in the Data Breach included Plaintiffs' and approximately 1.2 million other individuals' information (collectively "Patients").[4]

6. Defendant's failure to safeguard Patients' highly sensitive Private Information as

§ 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the subject data breach.

[2] https://www.tgh.org/cybersecurity-notice (last accessed Aug. 22, 2023) (the "Cybersecurity Notice").

[3] *Id.*

[4] https://www.wfla.com/news/hillsborough-county/1-2-million-affected-by-tampa-general-hospital-data-breach/ (last accessed Aug. 22, 2023).

exposed and unauthorizedly disclosed in the Data Breach violates its common law duty, Florida law, and Defendant's implied contract with its Patients to safeguard their Private Information.

7. Plaintiffs and Class members now face a lifetime risk of identity theft due to the nature of the information lost, including Social Security numbers, which they cannot change, and which cannot be made private again.

8. Defendant's harmful conduct has injured Plaintiffs and Class members in multiple ways, including, but not limited to: (i) the lost or diminished value of their Private Information; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive Private Information.

9. Defendant's failure to protect Patients' Private Information has harmed and will continue to harm approximately 1.2 million of Defendants' Patients, causing Plaintiffs to seek relief on a class wide basis.

10. On behalf of themselves and the Classes preliminarily defined below, Plaintiffs bring causes of action against Defendant for negligence, negligence *per se*, breach of implied contract, and violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201 *et seq.*, seeking an award of monetary damages and injunctive and declaratory relief, resulting from Defendant's failure to adequately protect their highly sensitive Private Information.

PARTIES

A. Plaintiffs

Angelica DiPierro

11. Plaintiff DiPierro is a resident and citizen of Florida.

12. Plaintiff DiPierro received health care services from Defendant.

13. Plaintiff DiPierro provided Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her Private Information.

14. If Plaintiff DiPierro had known that Defendant would not adequately protect her Private Information, she would not have allowed Defendant to maintain this sensitive Private Information.

Stacey Graham

15. Plaintiff Graham is a resident and citizen of Florida.

16. Plaintiff Graham received health care services from Defendant.

17. Plaintiff Graham provided Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her Private Information.

18. If Plaintiff Graham had known that Defendant would not adequately protect her Private Information, she would not have allowed Defendant to maintain this sensitive Private Information.

Deborah Ivey

19. Plaintiff Ivey is a resident and citizen of Florida.

20. Plaintiff Ivey received health care services from Defendant.

21. Plaintiff Ivey provided Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her Private Information.

22. If Plaintiff Ivey had known that Defendant would not adequately protect her Private Information, she would not have allowed Defendant to maintain this sensitive Private Information.

Edward James, Sr.

23. Plaintiff James is a resident and citizen of Florida.

24. Plaintiff James received health care services from Defendant.

25. Plaintiff James provided Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information.

26. If Plaintiff James had known that Defendant would not adequately protect his Private Information, he would not have allowed Defendant to maintain this sensitive Private Information.

Keon Critchlow

27. Plaintiff Critchlow is a resident and citizen of Florida.

28. Plaintiff Critchlow received health care services from Defendant.

29. Plaintiff Critchlow provided Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information.

30. If Plaintiff Critchlow had known that Defendant would not adequately protect his Private Information, he would not have allowed Defendant to maintain this sensitive Private Information.

Aubrey Rassel

31. Plaintiff Rassel is a resident and citizen of Florida.

32. Plaintiff Rassel received health care services from Defendant.

33. Plaintiff Rassel provided Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her Private Information.

34. If Plaintiff Rassel had known that Defendant would not adequately protect her Private Information, she would not have allowed Defendant to maintain this sensitive Private Information.

B. Defendant

35. Defendant is a corporation organized under the laws of Florida with its headquarters and principal place of business at 1 Tampa General Circle, Tampa, Florida 33606.

JURISDICTION AND VENUE

36. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

37. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District. Defendant has sufficient contacts in Florida, as it conducts a significant amount of its business in the State of Florida.

38. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL BACKGROUND

Defendant's Business

39. Defendant is a private not-for-profit hospital headquartered in Tampa, Florida, serving a dozen counties with a patient population of over 4 million people. As one of the largest hospital systems in Florida, Defendant is licensed for 1,040 beds, and with more than 8,000 team members, is one of the region's largest employers.[5]

40. Plaintiffs and Class members are current or former Patients of Defendant who provided their Private Information to Defendant.

41. To obtain medical services, Patients, including Plaintiffs and Class members, were required to provide sensitive and confidential Private Information, including their names, dates of birth, Social Security numbers, health records, insurance information, and other sensitive information, that would be held by Defendant in its computer systems.

42. The information held by Defendant at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class members.

43. Defendant made promises and representations to its Patients that the Private Information collected would be kept safe and confidential, the privacy of that information would be maintained, and Defendant would delete any sensitive information after it was no longer required to maintain it.

44. Indeed, Defendant's own Privacy Practices disclosure provides: "We are required by law to maintain the privacy of your PHI and to provide you with notice of our legal duties and privacy practices with respect to your PHI," and "We are committed to protecting the privacy of your health information."[6]

[5] https://www.tgh.org/about-tgh (last accessed Aug. 22, 2023).
[6] https://www.tgh.org/patients-visitors/joint-notice-privacy-policy (last accessed Aug. 22, 2023).

45. Plaintiffs and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access and disclosure.

46. Plaintiffs and Class members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

47. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class members from involuntary disclosure to third parties. Defendant has a legal duty to keep Patients' Private Information safe and confidential.

48. Defendant had obligations under the FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiffs and Class members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

49. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

50. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class members' Private Information from disclosure.

The Data Breach

51. On or about July 19, 2023, Defendant began notifying Patients of the Data Breach, informing them in an online "Cybersecurity Notice":

> Tampa General Hospital considers the health, safety, and privacy of our patients and team members a top priority. Regrettably, this notice concerns a cybersecurity event that may have involved some of that information.
>
> **What Happened?**
>
> On May 31, 2023, through our proactive monitoring tools, TGH detected unusual activity on our computer systems. We immediately took steps to contain the activity and began an investigation with the assistance of a third-party forensic firm. Fortunately, TGH's monitoring systems and experienced technology professionals effectively prevented encryption, which would have significantly interrupted the hospital's ability to provide care for patients. However, the investigation determined that an unauthorized third party accessed TGH's network and obtained certain files from its systems between May 12 and May 30, 2023.
>
> TGH reported the event to the FBI and provided information to support its investigation of the criminal group responsible.
>
> **What Information Was Involved?**
>
> We reviewed the files involved and determined that some patient information was included. The information varied by individual, but may have included names, addresses, phone numbers, dates of birth, Social Security numbers, health insurance information, medical record numbers, patient account numbers, dates of service and/or limited treatment information used by TGH for its business operations. TGH's electronic medical record system was not involved or accessed.
>
> **What is TGH Doing?**
>
> TGH considers the health, safety and privacy of patients and team members a top priority. The hospital is continuously updating and hardening systems to help prevent events such as this from occurring and has implemented additional defensive tools and increased monitoring.
>
> **What Can Patients Do?**
>
> TGH will be mailing notification letters to individuals whose information may have been involved in this event and is also providing individuals whose Social Security number was involved with complimentary credit monitoring and identity theft protection services. Patients are encouraged to review statements from their health

> insurer and healthcare providers, and to contact them immediately if they see any services they did not receive.[7]

52. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive and confidential Private Information it was maintaining for Plaintiffs and Class members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

53. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiffs and Class members, including their names, addresses, phone numbers, dates of birth, Social Security numbers, health insurance information, medical record numbers, patient account numbers, dates of service and/or treatment information. Plaintiffs' and Class members' Private Information was accessed and stolen in the Data Breach.

54. Plaintiffs further believe their Private Information, and that of Class members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' Private Information.

55. As alleged above, as a condition to obtain medical services from Defendant, Plaintiffs and Class members were required to give their sensitive and confidential Private Information to Defendant.

56. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class members.

[7] *See* Cybersecurity Notice.

57. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk of a Cyber Attack Because Healthcare Entities in Possession of Private Information Are Particularly Suspectable to Cyber Attacks.

58. Data thieves regularly target entities in the healthcare industry like Defendant due to the highly sensitive information that they maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

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

60. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

61. For example, of the 1,862 recorded data breaches in 2021, 330 of them, or 17.7%, were in the medical or healthcare industry.[8]

[8] 2021 Data Breach Annual Report (ITRC, Jan. 2022), https://notified.idtheftcenter. org/s/, at 6.

62. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[9]

63. Entities in custody of PHI reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[10] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[11] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.[12]

64. Despite the prevalence of public announcements of data breach and data security compromises in the healthcare industry, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class members from being compromised in the Data Breach.

65. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to over one million individuals'

---

[9] *Id.*
[10] *See* Identity Theft Resource Center, *2022 Annual Data Breach Report*, https://www.idtheftcenter.org/publication/2022-data-breach-report/ (last accessed Aug. 22, 2023).
[11] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Aug. 22, 2023).
[12] *See id.*

detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

66. In its Cybersecurity Notice, Defendant says it will be "providing individuals whose Social Security number was involved with complimentary credit monitoring and identity theft protection services."[13] This is wholly inadequate to compensate Plaintiffs and Class members, as it fails to account for the multiple years of ongoing identity theft and financial fraud commonly faced by victims of data breaches and other unauthorized disclosures. It also fails to provide sufficient compensation to Plaintiffs and Class members for the unauthorized release and disclosure of their Private Information. Moreover, once the identity theft service expires, Plaintiffs and Class members will be forced to pay out of pocket for necessary identity monitoring services.

67. Defendant's offering of identity theft protection establishes that Plaintiffs' and Class members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems. Moreover, Defendant's offer indicates that it recognizes Plaintiffs and Class members are at a present and continuing risk of identity theft and fraud as a result of the Data Breach.

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

69. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

[13] *See* Cybersecurity Notice.

70. As a healthcare entity in possession of its Patients' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class members because of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Defendant Fails to Comply with FTC Guidelines

71. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, data security needs should be factored into all business decision-making.

72. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note businesses should protect the personal 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 to correct any security problems.[14]

73. The guidelines also recommend 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.[15]

[14] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Aug. 22, 2023).
[15] *Id.*

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

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

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

77. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

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

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

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

Defendant Fails to Comply with HIPAA Guidelines.

81. Defendant is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy 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.

82. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[16] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

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

84. 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.

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

86. "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.

87. 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 its workforce.

45 C.F.R. Part 160 and Part 164, Subparts A and C.

88. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to

those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

89. HIPAA and HITECH also obligate Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic PHI 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.

90. 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).

91. 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 PHI 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).

92. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[17] The list of resources includes a link to guidelines set by the National Institute of

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

Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[18]

Defendant Owed Plaintiffs and Class Members a Common Law Duty to Safeguard their Private Information.

93. In addition to its obligations under federal and state laws, Defendant owed a common law duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a common law duty to Plaintiffs 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 Private Information of Class members.

94. Defendant owed a common law duty to Plaintiffs and Class members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

95. Defendant owed a common law duty to Plaintiffs and Class members to implement processes that would detect a compromise of Private Information in a timely manner.

96. Defendant owed a common law duty to Plaintiffs and Class members to act upon data security warnings and alerts in a timely fashion.

97. Defendant owed a common law duty to Plaintiffs and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

[18] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed Aug. 22, 2023).

98. Defendant owed a common law duty of care to Plaintiffs and Class members because they were foreseeable and probable victims of any inadequate data security practices.

The Data Breach Increases Plaintiffs' and Class Members' Risk of Identity Theft.

99. Plaintiffs believe their unencrypted Private Information was sold on the dark web following the Data Breach, as that is the *modus operandi* of hackers.

100. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class members.

101. Simply put, unauthorized individuals can easily access the Private Information of Plaintiffs and Class members because of the Data Breach.

102. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

103. Plaintiffs' and Class members' Private Information is of great value to hackers and cyber criminals, and, as alleged below, the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class members and to profit from their misfortune.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

104. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous

situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

105. Thus, due to the actual, present, and continuing risk of identity theft, Plaintiffs and Class members must, as Defendant's Cybersecurity Notice encourages them to, "review statements from their health insurer and healthcare providers, and to contact them immediately if they see any services they did not receive."[19] They must also monitor their financial accounts for many years to mitigate the risk of identity theft.

106. Plaintiffs and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems.

107. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[20]

108. Plaintiffs' mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports,

[19] *See* Cybersecurity Notice.

[20] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed Aug. 22, 2023).

contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[21]

109. And for those Class members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

Diminution of Value of Private Information.

110. Private Information is valuable property.[22] Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber theft include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that Private Information has considerable market value.

111. The Private Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach—most notably name and Social Security number—is difficult, if not impossible, to change.

112. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black

[21] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed Aug. 22, 2023).
[22] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed Aug. 22, 2023) ("GAO Report").

market."[23]

113. Sensitive Private Information could sell for as much as $363 per record according to the Infosec Institute in 2009.[24]

114. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[25] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[26,27] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[28]

115. As a result of the Data Breach, Plaintiffs' and Class members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class members for their property, resulting in an

[23] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Aug. 22, 2023).

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

[25] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed Aug. 22, 2023).

[26] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed Aug. 22, 2023).

[27] https://datacoup.com/ (last accessed Aug. 22, 2023).

[28] https://www.thepennyhoarder.com/make-money/nielsen-panel/#:~:text=Sign%20up%20to%20join%20the,software%20installed%20on%20your%20computer (last accessed Aug. 22, 2023).

economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

116. Fraudulent activity resulting from the Data Breach may not come to light for years.

117. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

118. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to over a million individuals' detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary.

120. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, Plaintiffs believe entire batches of stolen information have been or will be placed on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; obtaining health care services; or filing false unemployment claims.

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

122. Consequently, Plaintiffs and Class members face and will continue to face a substantial risk of fraud and identity theft for the remainder of their lifetimes.

123. The retail cost of credit monitoring and identity theft monitoring is approximately $200.00 a year per Class member. This is a reasonable and necessary cost to monitor and protect Class members from the risk of identity theft resulting from Defendant's Data Breach. This is a future cost that Plaintiffs and Class members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss of the Benefit of the Bargain

124. Furthermore, Defendant's poor data security deprived Plaintiffs and Class members of the benefit of their bargain. When agreeing to pay Defendant for the provision of its health care services, Plaintiffs and other reasonable consumers understood and expected they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiffs' Experiences

Angelica DiPierro

125. Plaintiff DiPierro obtained medical services from Defendant. To obtain these medical services, she was required to provide her Private Information to Defendant.

126. Upon information and belief, at the time of the Data Breach—between May 12, 2023, and May 30, 2023—Defendant retained Plaintiff DiPierro's Private Information in its system.

127. Plaintiff DiPierro is very careful about sharing her sensitive Private Information. Plaintiff DiPierro stores any documents containing her Private Information in a safe and secure location. Plaintiff DiPierro has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

128. Plaintiff DiPierro received a letter from Defendant concerning the Data Breach. According to the letter, Plaintiff DiPierro's Private Information was improperly accessed and obtained by unauthorized third parties. The Private Information comprised some combination of her name, address, telephone number, date of birth, Social Security number, health insurance information, medical record number, patient account number, dates of service, and/or limited information related to treatment received at TGH used by Defendant for its business operations.

129. As a result of the Data Breach, Plaintiff DiPierro has made reasonable efforts to mitigate the impact of the Data Breach. She spends approximately 20 minutes, every other day, reviewing her accounts for fraud and identity theft. Plaintiff DiPierro has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be

recaptured. Plaintiff DiPierro anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach.

130. As a result of the Data Breach, Plaintiff DiPierro fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

131. As a result of the Data Breach, Plaintiff DiPierro is presently at risk and will continue to be at increased risk of identity theft and fraud for the remainder of her lifetime.

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

Stacey Graham

133. Plaintiff Graham obtained medical services from Defendant. To obtain these medical services, she was required to provide her Private Information to Defendant.

134. Upon information and belief, at the time of the Data Breach—between May 12, 2023, and May 30, 2023—Defendant retained Plaintiff Graham's Private Information in its system.

135. Plaintiff Graham is very careful about sharing her sensitive Private Information. Plaintiff Graham stores any documents containing her Private Information in a safe and secure location. Plaintiff Graham has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

136. Plaintiff Graham received a letter from Defendant concerning the Data Breach. According to the letter, Plaintiff Graham's Private Information was improperly accessed and

obtained by unauthorized third parties. The Private Information comprised some combination of her name, address, phone number, date of birth, Social Security number, health insurance information, medical record number, patient account number, dates of service, and/or limited information related to treatment received at TGH used by Defendant for its business operations.

137. As a result of the Data Breach, Plaintiff Graham has made reasonable efforts to mitigate the impact of the Data Breach. She has spent a minimum of half an hour monitoring her accounts. She has also experienced an increase in the number of intrusive spam calls and texts she receives. Plaintiff Graham has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff Graham anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach.

138. As a result of the Data Breach, Plaintiff Graham fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

139. As a result of the Data Breach, Plaintiff Graham is presently at risk and will continue to be at increased risk of identity theft and fraud for the remainder of her lifetime.

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

Deborah Ivey

141. Plaintiff Ivey obtained medical services from Defendant. To obtain these medical services, she was required to provide her Private Information to Defendant.

142. Upon information and belief, at the time of the Data Breach—between May 12, 2023, and May 30, 2023—Defendant retained Plaintiff Ivey's Private Information in its system.

143. Plaintiff Ivey is very careful about sharing her sensitive Private Information. Plaintiff Ivey stores any documents containing her Private Information in a safe and secure location. Plaintiff Ivey has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

144. Plaintiff Ivey received a letter from Defendant concerning the Data Breach. According to the letter, Plaintiff Ivey's Private Information was improperly accessed and obtained by unauthorized third parties. The Private Information comprised some combination of her name, address, phone number, date of birth, Social Security number, health insurance information, medical record number, patient account number, dates of service, and/or limited information related to treatment received at TGH used by Defendant for its business operations.

145. As a result of the Data Breach, Plaintiff Ivey has made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Ivey has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff Ivey anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach.

146. As a result of the Data Breach, Plaintiff Ivey fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is

experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

147. As a result of the Data Breach, Plaintiff Ivey is presently at risk and will continue to be at increased risk of identity theft and fraud for the remainder of her lifetime.

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

Edward James, Sr.

149. Plaintiff James obtained medical services from Defendant. To obtain these medical services, he was required to provide his Private Information to Defendant.

150. Upon information and belief, at the time of the Data Breach—between May 12, 2023, and May 30, 2023—Defendant retained Plaintiff James' Private Information in its system.

151. Plaintiff James is very careful about sharing his sensitive Private Information. Plaintiff James stores any documents containing his Private Information in a safe and secure location. Plaintiff James has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

152. Plaintiff James received a letter from Defendant concerning the Data Breach. According to the letter, Plaintiff James' Private Information was improperly accessed and obtained by unauthorized third parties. The Private Information comprised some combination of his name, address, phone number, date of birth, Social Security number, health insurance information, medical record number, patient account number, dates of service, and/or limited information related to treatment received at TGH used by Defendant for its business operations.

153. Plaintiff James has been the victim of fraud as a result of the Data Breach. Since the Data Brach, Plaintiff James discovered a fraudulent charge to his bank account in the amount of $2,600.70 for the purchase of a television. Additionally, there have been two unauthorized ATM withdrawals in the amount of $400 each from his bank account.

154. As a result of the Data Breach, Plaintiff James has made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff James has spent significant time dealing with the Data Breach, including contacting his bank regarding the fraudulent charges referenced above, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff James anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach.

155. As a result of the Data Breach, Plaintiff James fears for his personal financial security and uncertainty over what medical information was revealed in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

156. As a result of the Data Breach, Plaintiff James is presently at risk and will continue to be at increased risk of identity theft and fraud for the remainder of his lifetime.

157. Plaintiff James has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Keon Critchlow

158. Plaintiff Critchlow obtained medical services from Defendant. To obtain these medical services, he was required to provide his Private Information to Defendant.

159. Upon information and belief, at the time of the Data Breach—between May 12, 2023, and May 30, 2023—Defendant retained Plaintiff Critchlow's Private Information in its system.

160. Plaintiff Critchlow is very careful about sharing his sensitive Private Information. Plaintiff Critchlow stores any documents containing his Private Information in a safe and secure location. Plaintiff Critchlow has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

161. Plaintiff Critchlow received a letter from Defendant concerning the Data Breach. According to the letter, Plaintiff Critchlow's Private Information was improperly accessed and obtained by unauthorized third parties. The Private Information comprised some combination of his name, address, phone number, date of birth, Social Security number, health insurance information, medical record number, patient account number, dates of service, and/or limited information related to treatment received at TGH used by Defendant for its business operations.

162. As a result of the Data Breach, Plaintiff Critchlow has made reasonable efforts to mitigate the impact of the Data Breach. He has spent at least 3.5 hours monitoring his accounts and contacting Defendant to seek information about the Data Breach. He has also experienced an increase in the number of intrusive spam calls and texts he receives. Plaintiff Critchlow has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever

and cannot be recaptured. Plaintiff Critchlow anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach.

163. As a result of the Data Breach, Plaintiff Critchlow fears for his personal financial security and uncertainty over what medical information was revealed in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

164. As a result of the Data Breach, Plaintiff Critchlow is presently at risk and will continue to be at increased risk of identity theft and fraud for the remainder of his lifetime.

165. Plaintiff Critchlow has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Aubrey Rassel

166. Plaintiff Rassel obtained medical services from Defendant. To obtain these medical services, she was required to provide her Private Information to Defendant.

167. Upon information and belief, at the time of the Data Breach—between May 12, 2023, and May 30, 2023—Defendant retained Plaintiff Rassel's Private Information in its system.

168. Plaintiff Rassel is very careful about sharing her sensitive Private Information. Plaintiff Ivey stores any documents containing her Private Information in a safe and secure location. Plaintiff Ivey has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

169. Plaintiff Rassel received a letter from Defendant concerning the Data Breach. According to the letter, Plaintiff Rassel's Private Information was improperly accessed and

obtained by unauthorized third parties. The Private Information comprised some combination of her name, address, phone number, date of birth, Social Security number, health insurance information, medical record number, patient account number, dates of service, and/or limited information related to treatment received at TGH used by Defendant for its business operations.

170. As a result of the Data Breach, Plaintiff Rassel has made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Rassel has also experienced an increase in the number of intrusive spam calls and texts she receives. Plaintiff Rassel has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff Rassel anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach.

171. As a result of the Data Breach, Plaintiff Rassel fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

172. As a result of the Data Breach, Plaintiff Rassel is presently at risk and will continue to be at increased risk of identity theft and fraud for the remainder of her lifetime.

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

CLASS ACTION ALLEGATIONS

174. Pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiffs bring this action on behalf of themselves and on behalf of all members of the proposed Nationwide Class and Florida Subclass (collectively the "Class" or "Classes") defined as:

> **Nationwide Class:** All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported to have occurred on or about between May 12, 2023, and May 30, 2023.
>
> **Florida Subclass:** All individuals residing in the State of Florida whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported to have occurred on or about between May 12, 2023, and May 30, 2023.

175. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

176. Plaintiffs reserve the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

177. **Numerosity**: The Class members are so numerous that joinder of all members is impracticable, if not completely impossible. Approximately 1.2 million individuals were affected by the of the Data Breach. The Class is apparently identifiable within Defendant's records, and Defendant intends to identify these individuals (as stated in the Cybersecurity Notice).

178. **Commonality and Predominance:** Common questions of law and fact exist as to all Class members and predominate over any questions affecting solely individual Class members.

Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, are the following:

a. Whether and to what extent Defendant had statutory and common law duties to protect the Private Information of Plaintiffs and Class members;

b. Whether Defendant had respective duties not to disclose or allow to be disclosed the Private Information of Plaintiffs and Class members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the Private Information of Plaintiffs and Class members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class members;

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

f. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Plaintiffs and Class members are entitled to actual damages and/or nominal damages as a result of Defendant's wrongful conduct; and

h. Whether Plaintiffs and Class members are entitled to declaratory and/or injunctive relief to redress the present and continuing harm faced as a result of the Data Breach.

i. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

j. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

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

l. Whether Defendant's failure to institute adequate protective security measures amounted to breach of an implied contract;

m. Whether Defendant's failure to institute adequate protective security measures violated FDUTPA;

n. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

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

179. **Typicality**: Plaintiffs' claims are typical of those of the other Class members because Plaintiffs, like every other Class member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Classes.

180. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of Class members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class members. Plaintiffs seek no relief that is antagonistic or adverse to Class members and the infringement of the rights and the damages they have suffered are typical of other Class members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

181. **Superiority**: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that millions of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

182. The nature of this action and the nature of laws available to Plaintiffs and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

183. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

184. **Equitable Relief:** This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final declaratory and injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

185. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in paragraphs 1 through 184.

186. Defendant requires its Patients, including Plaintiffs and Class members, to submit non-public Private Information in the ordinary course of providing health plan services.

187. Defendant gathered and stored the Private Information of Plaintiffs and Class members as part of its business of soliciting its services to its Patients, which solicitations and services affect commerce.

188. Plaintiffs and Class members entrusted Defendant with their Private Information with the understanding Defendant would safeguard their information.

189. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm Plaintiffs and Class members could and would suffer if the Private Information were wrongfully disclosed.

190. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period-of-time and to give prompt notice to those affected in the case of a data breach.

191. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

193. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its Patients. That special relationship arose because Plaintiffs and Class members entrusted Defendant with their confidential Private Information, a necessary part of being Patients of Defendant.

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

195. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

196. Defendant breached its duties, thus was negligent, by failing to use reasonable measures to protect Class members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, (a) failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information; (b) failing to adequately monitor the security of their networks and systems; and (c) allowing unauthorized access to Class members' Private Information.

197. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly considering Defendant's inadequate security practices.

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

199. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class members could and would suffer if the Private Information were wrongfully disclosed.

200. Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the

inherent risks in collecting and storing the Private Information of Plaintiffs and Class members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

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

202. Plaintiffs and Class members had no ability to protect their Private Information that was in, and likely remains in, Defendant's possession.

203. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

204. Defendant's duty extended to protecting Plaintiffs and Class members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard Private Information.

205. Defendant has admitted that the Private Information of Plaintiffs and Class members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

206. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class members, the Private Information of Plaintiffs and Class members would not have been compromised.

207. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class members and the

present and continuing risk of fraud and identity theft suffered by Plaintiffs and Class members. The Private Information of Plaintiffs and Class members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

208. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members have suffered and will continue to suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

209. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

210. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

211. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiffs and the Nationwide Class)

212. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in paragraphs 1 through 184.

213. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

214. Defendant is covered by HIPAA (*see* 45 C.F.R. § 160.102) and as such 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.

215. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

216. Among other things, HIPAA limits the permissible uses of PHI and prohibits unauthorized disclosures of PHI.

217. HIPAA requires that Defendant implement appropriate safeguards for this information.

218. Defendant breached its duties to Plaintiffs and Class members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

219. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

220. The injuries to Plaintiffs and Class members resulting from the Data Breach were directly and indirectly caused by Defendant's violation of the statutes described herein.

221. Plaintiffs and Class members were within the class of persons the FTC Act and HIPAA are intended to protect and the type of harm that resulted from the Data Breach is the type of harm these statutes are intended to guard against.

222. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

223. The injuries and harms suffered by Plaintiffs and Class members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that Defendant's breach would cause Plaintiffs and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

224. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class members have suffered injuries and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract and Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the Nationwide Class)

225. Plaintiffs re-allege and incorporate by reference herein all of the allegations

contained in paragraphs 1 through 184.

226. Defendant offered to provide services to its Patients, including Plaintiffs and Class members, in exchange for payment.

227. Defendant also required Plaintiffs and the Class members to provide Defendant with their Private Information to receive services.

228. In turn, Defendant impliedly promised to protect Plaintiffs' and Class members' Private Information through adequate data security measures.

229. Plaintiffs and the Class members accepted Defendant's offer by providing Private Information to Defendant in exchange for receiving Defendant's services, and then by paying for and receiving the same.

230. Plaintiffs and Class members would not have entrusted their Private Information to Defendant but for the above-described agreement with Defendant.

231. Defendant materially breached its agreement(s) with Plaintiffs and Class members by failing to safeguard such Private Information, violating industry standards necessarily incorporated in the agreement.

232. Plaintiffs and Class members have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

233. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along

with its form.

234. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

235. The losses and damages Plaintiffs and Class members sustained as described herein were the direct and proximate result of Defendant's breach of the implied contracts with them, including breach of the implied covenant of good faith and fair dealing.

COUNT IV
Violation of the Florida Deceptive and Unfair Trade Practices Act,
Fla. Stat. § 501.201 *et seq.*
(On behalf of Plaintiffs and the Florida Subclass)

236. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 184.

237. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, *et seq.* ("FDUTPA") provides that "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."

238. In connection with providing services involving Private Information, Defendant represented, directly or indirectly, expressly or by implication to consumers, including Plaintiffs and the proposed Florida Subclass members, that it would safeguard their Private Information entrusted to Defendant, including but limited to, by undertaking adequate security measures consistent with industry standards, and by adequately training employees.

239. As alleged above, Defendant knew or should have known that its data security measures were inadequate.

240. As a result, Defendant's representations of undertaking adequate data security measures and training measures to safeguard Plaintiffs' and the proposed Florida Subclass

members' Private Information as set forth above were false and misleading and constitute deceptive acts or practices in violation of § 501.204, Fla. Stat.

241. As a result of the above violations of FDUTPA, Plaintiffs and the proposed Florida Subclass members have suffered injury and damages as set forth herein.

242. Plaintiffs and the Florida Subclass members are also entitled to declaratory and injunctive relief pursuant to § 501.211, Fla. Stat.

243. Plaintiffs have retained the undersigned counsel to prosecute this action and are entitled to recover their attorneys' fees and costs pursuant to § 501.2105, Fla. Stat.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class members, request judgment against Defendant and that the Court grant the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. For a judgement declaring, among other things, the following:

i. Defendant owes a legal duty to secure Plaintiffs' and Class members' Private Information under the common law, HIPAA, the FTCA, and other state and federal laws and regulations set forth herein;

ii. Defendant's existing data monitoring measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect individuals' Private Information; and

iii. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and Class members' Private Information.

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs 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 Private Information of Plaintiffs 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 Plaintiffs and Class members;

iv. requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class members 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 security checks;

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 Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct an 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.

D. For an award of damages, including actual, nominal, punitive, and consequential damages, as allowed by law in an amount to be determined by a jury at trial;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: August 22, 2023.

Respectfully submitted,

By: *Jeff Ostrow*
Jeff Ostrow FBN 121452
Kristen Lake Cardoso FBN 44401
Steven Sukert FBN 1022912
KOPELOWITZ OSTROW
FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
ostrow@kolawyers.com
cardoso@kolawyers.com
sukert@kolawyers.com

Attorneys for Plaintiffs and the Putative Classes