FILED
2025 Jun-11 PM 02:56
U.S. DISTRICT COURT
N.D. OF ALABAMA

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA

F.P. AND C.W., INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, Plaintiffs, v. **ADDICTION AND MENTAL HEALTH SERVICES, LLC D/B/A BRADFORD HEALTH SERVICES,** Defendant.	Civil Action No.: _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff F.P. and Plaintiff C.W. (together "Plaintiffs"), by and through the undersigned counsel, brings this class action complaint against Defendant Addiction and Mental Health Services, LLC d/b/a Bradford Health Services ("Bradford" or "Defendant"), on behalf of themselves and all others similarly situated. Plaintiffs make the following allegations based upon personal knowledge as to their own actions and upon information and belief as to all other matters:

INTRODUCTION

1. Bradford is a recognized provider of comprehensive substance abuse treatment and recovery services throughout the southeastern United States, with

28 facilities across six states, including Alabama, Florida, Mississippi, North Carolina, Tennessee, and Texas.

2. Bradford provides a comprehensive range of services including early intervention services, crisis response, intensive outpatient care, partial hospitalization, and residential care, inpatient detox, and transitional living and life skills programming – all designed to help those struggling with substance abuse recover is a structured, safe, secure, and privacy-preserving environment – and all involving the collection and maintenance of troves of highly sensitive personal and medical information.

3. Bradford recognizes that the information it collects from patients is of a highly private and sensitive nature, and acknowledges its legal duty to safeguard that information.

4. In its Notice of Privacy Practices, Bradford expressly states that it is "required by law to maintain the privacy and security of your Protected Health Information and records;" and that it is "required to notify you if there is a breach of your unsecured Protected Health Information or unsecured records."[1]

5. Yet Bradford failed to comply with both of these legal obligations, leaving Bradford's current and former patients and employees suffering the

[1] *See* https://bradfordhealth.com/notice-of-privacy-practices

ongoing, long- term effects of a data breach Defendant hid from them for more than eighteen months.

6. On December 8, 2023, Bradford discovered that it was the subject of a massive data breach whereby hackers gained unauthorized access to its networks (the "Data Breach").[2]

7. Bradford then purposely hid that knowledge for over eighteen months.

8. On May 30, 2025, Bradford posted a Notice of Data Security Incident ("Notice") on its website, disclosing the Data Breach for the first time.[3]

9. Bradford explained that after investigating the Data Breach, it "determined that certain individuals' personal and/or protected health information may have been affected." The affected information includes "individuals' names, driver's license numbers, dates of birth, medical information (including diagnosis and treatment information, physician names, and Medical Record numbers), health insurance information, financial account numbers, passport numbers, payment card numbers plus a means of access to the account, and/or Social Security numbers."[4]

---

[2] *See* https://bradfordhealth.com/notice-of-data-security-incident/

[3] *Id.*

[4] *Id.*

10. The Notice leaves more questions open than it answers.

11. Bradford claims in the Notice it "has implemented additional measures to enhance network security and minimize the risk of a similar incident occurring in the future," but does not say what those measures are or explain how those measures minimize that risk.[5]

12. Bradford claims, without providing any support, that it "has no evidence that the information potentially involved in this incident has been misused," but fails to explain what evidence, if any, Bradford actually looked for.[6]

13. Bradford also fails to provide any explanation or justification for waiting over eighteen months to notify affected individuals that they were victims of the Data Breach and needed to take steps to protect themselves.

14. On May 30, 2025, Bradford provided written notification of the incident via U.S. mail to impacted individuals.[7]

15. Upon information and belief, personal and/or protected health information of both Bradford's current and former patients, and of its current and former employees was compromised in the Data Breach.

[5] *See* https://bradfordhealth.com/notice-of-data-security-incident/

[6] *Id.*

[7] *Id.*

16. Upon information and belief, Bradford failed to notify the relevant government officials of the Data Breach at the time Bradford first discovered the Data Breach.

17. Upon information and belief, Bradford first notified the relevant government officials of the Data Breach on or about the time it posted the Notice of Security Incident on its website.

18. The cybergroup Hunters International has claimed responsibility for the Data Breach, boasting that they exfiltrated 760GB of data from Bradford's systems.[8]

19. Hunters International is a prominent Ransomware-as-a-Service (RaaS) operation. Until late 2024, Hunters International operated under a ransomware-and-extortion model. In January 2025, Hunters International rebranded itself as World Leaks, and now focuses solely on data extortion.[9]

20. As of July 2024, Hunters International successfully compromised victims in at least 29 countries.[10] Unlike many other ransomware groups which use

[8] *Id*.

[9] Andrew Doyle, April 4, 2025, *Hunters International Shifts to Data Extortion and Rebrands as World Leaks*, Security Spotlight (April 4, 2025) at https://dailysecurityreview.com/security-spotlight/hunters-international-shifts-to-data-extortion-and-rebrands-as-world-leaks/

[10] Christine Barry, *Hunters International: Your data is the prey*, Barracuda Blog (July 29, 2024) at https://blog.barracuda.com/2024/07/29/hunters-international--your-data-is-the-prey

the compromised data they obtain as secondary leverage, data exfiltration and use of that data is Hunters International's top priority.[11]

21. Hunters International also has no qualms about releasing and using highly sensitive data obtained from its ransomware attacks. For example, following its ransomware attack on a US plastic surgeon's clinic, Hunters International leaked patients' pre-operation pictures to expedite ransom payments.[12]

22. Hunters International's amoral tactics are especially relevant here given the vulnerable population served by Bradford and the increased risk of harm to that population whose highly sensitive PII and PHI was exfiltrated in the Data Breach.

23. Bradford's eighteen month cover up of the Data Breach is especially egregious given the patient population Bradford serves.

24. Bradford "provides addiction treatment programs, resources, and community for every aspect of recovery," through its "premier drug and alcohol rehab facilities across the Southeast."[13] Bradford describes itself as "more than a

[11] *Id*.

[12] *Threat Actor Profile: Hunters International Ransomware Group*, Threat Analyst (November 22, 2023), at https://www.threatintelreport.com/2023/11/22/threat_actor_profiles/threat-actor-profile-hunters-international-ransomware-group/

[13] *See* https://bradfordhealth.com/

healthcare network; we are recovery communities for every stage of the journey."[14] Since its founding in 1977, Bradford "has treated nearly half a million patients through a wide array of innovative and effective recovery programs."[15]

25. Hunters International accessed, copied, and exfiltrated highly sensitive personal identifying information ("PII") and personal health information ("PHI") (together "Private Information") stored on Defendant's servers including names, driver's license numbers, dates of birth, medical information, health insurance information, financial account numbers, passport numbers, social security numbers ("SSNs"), and payment card numbers along with a means of access to the payment card accounts.[16]

26. PHI is considered "the most confidential and valuable type of [PII] . . . irrevocable once breached."[17]

---

[14] *Id.*

[15] *See* https://bradfordhealth.com/treatment-programs/

[16] *MMRG Notifies Patients of Cybersecurity Incident*, BUSINESS WIRE (Feb. 6, 2024), https://www.businesswire.com/news/home/20240206060527/en/.

[17] Junyuan Ke, et al., *My Data or My Health? Heterogenous Patient Responses to Healthcare Data Breach*, SSRN (Feb. 10, 2022), http://dx.doi.org/10.2139/ssrn.4029103. Under the Health Insurance Portability and Accountability Act, 42 U.S.C. §§1320d, et seq. ("HIPAA"), PHI is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. §160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. Summary

27. Plaintiffs' and Class Members' identities have been and continue to be at a heightened risk of exposure because of Defendant's negligent conduct since Private Information that Defendant collected from them and stored is now in the hands of data thieves.

28. Armed with the Private Information accessed in the Data Breach, data thieves can now use the PII and PHI obtained from Defendant to commit a variety of crimes, including credit/debit card fraud, tax fraud, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' names to set up utility accounts, using Class Members' health information to target other phishing and hacking intrusions based upon their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

29. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of

---

of the HIPAA Privacy Rule, U.S. DEP'T OF HEALTH & HUMAN SERS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited March 28, 2024).

dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

30. As a direct result of the Data Breach, Plaintiffs and Class Members have suffered fraud and will continue to be exposed to a heightened and imminent risk of fraud and identity theft, including medical fraud, potentially for the rest of their lives. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft, and their medical accounts to guard against medical identity theft.

31. Plaintiffs and Class Members are also at an ongoing, increased risk of extortion and blackmail given the sensitive nature of addiction treatment and cybercriminals' ability to use Plaintiffs' and Class Members' compromised data from Bradford against them.

32. Plaintiffs and Class Members may also incur out-of-pocket costs for purchasing credit monitoring services, identity theft protection services, credit freezes, credit reports, and other protective measures to deter and detect identity theft.

33. As a direct and proximate result of the Data Breach and subsequent exposure of their Private Information, Plaintiffs and Class Members also suffered additional ascertainable losses, including, but not limited to, a loss of the value of their private and confidential information, and the loss of the benefit of their contractual bargain with Defendant.

34. As a direct and proximate result of the Data Breach and subsequent exposure of their Private Information, Plaintiffs and Class Members have suffered, and will continue to suffer damages and economic losses in the form of lost time needed to take appropriate measures to avoid unauthorized and fraudulent charges, putting alerts on their credit files, and dealing with spam phone calls, letters, and emails received as a result of the Data Breach.

35. As a direct and proximate result of the Data Breach and subsequent exposure of their Private Information, Plaintiffs and Class Members have suffered, and will continue to suffer, an invasion of their property interest in their own PII and PHI such that they are entitled to damages from Defendant for unauthorized access to, theft of, and misuse of their Private Information. These harms are ongoing, and Plaintiffs and Class Members will suffer from future damages associated with the unauthorized use and misuse of their Private Information as thieves will continue to use the information to obtain money and credit in their names for several years.

36. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed via and/or compromised during the Data Breach.

37. Defendant is responsible for the Data Breach because Defendant failed to implement reasonable security procedures and practices and failed to disclose material facts surrounding Defendant's deficient security protocols.

38. As a result of Defendant's failure to protect the sensitive information Defendant was entrusted to safeguard, Plaintiffs and Class Members did not receive the benefit of their bargain with Defendant and now face a significant risk of medical-related theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

39. As a result of Defendants unreasonably and intentionally delaying disclosure of the Data Breach, Plaintiffs and Class Members were left without the knowledge that their Private Information had been compromised by cybercriminals, and that there were steps they should take to protect themselves from the resulting risk of harm including medical-related theft and fraud, financial fraud, and other identity-related fraud.

PARTIES

40. Plaintiff F.P. is a citizen and resident of Birmingham, Alabama.

41. Plaintiff C.W. is a citizen and resident of Florida.

42. Defendant Addiction and Mental Health Services, LLC d/b/a Bradford Heath Services is a Delaware limited liability company with its principal place of business in Birmingham, Alabama, making Defendant a citizen of Delaware and Alabama for purposes of the Class Action Fairness Act. *See* 28 U.S.C. 1332(d)(10). *See also*, *Griggs v. NHS Mgmt. LLC*, No. 2:22-CV-00565-RDP, 2023 WL 4190535, at *3 (N.D. Ala. June 26, 2023) ("The normal rule regarding citizenship of a limited liability company does not apply in CAFA cases. Instead, CAFA provides that 'an unincorporated association shall be deemed to be a citizen of the State where it has its principal place of business and the State under whose laws it is organized.'" (quoting 28 U.S.C. § 1332(d)(10)).

JURISDICTION AND VENUE

43. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members and Plaintiff C.W. as well as at least some members of the proposed Class have a different citizenship from Defendant. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

44. This Court has general and specific personal jurisdiction over Defendant because Defendant maintains and operate its headquarters in this

District and/or is authorized to and do conduct business in this District; and because the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

45. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) (1) & (2) because Defendant resides in this District and/or a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Data Collection and Privacy Practices

46. Bradford provides comprehensive substance abuse treatment and recovery services throughout the southeastern United States, including Alabama, Florida, Mississippi, North Carolina, Tennessee, and Texas.

47. Defendant's current and former patients reside throughout the United States.

48. In the regular course of business, Defendant collects and stores patients' highly sensitive PII and PHI including their names, addresses, driver's license numbers, dates of birth, medical information (including diagnosis and treatment information, physician names, and Medical Record numbers), health insurance information, financial account numbers, passport numbers, payment card numbers plus a means of access to the account, and Social Security numbers, and much more.

49. Bradford expressly states that it is "required by law to maintain the privacy and security of your Protected Health Information and records;" and that it is "required to notify you if there is a breach of your unsecured Protected Health Information or unsecured records."

50. Through the possession and utilization of Plaintiffs' and Class Members' Private Information, Defendant assumed duties owed to Plaintiffs and Class Members regarding their Private Information. Therefore, Defendant knew or should have known that it was responsible for safeguarding Plaintiffs' and Class Members' Private Information from unauthorized access and criminal misuse.

51. Defendant is a covered entity under HIPAA.

52. As a HIPAA covered entity, Defendant was required to protect against reasonably anticipated threats to the security of PHI. Defendant was also required to implement safeguards to ensure the confidentiality, integrity, and availability of PHI.

53. Given Defendant's representations and experience handling highly sensitive PHI and other Private Information, Defendant understood the need to protect patients' PHI and other Private Information and prioritize data security.

54. Plaintiffs and Class Members relied on Defendant to keep their Private Information secure and safeguarded for authorized purposes. Defendant

owed a duty to Plaintiffs and Class Members to secure their Private Information as such, and ultimately breached that duty.

The Data Breach

55. On December 8, 2023, Defendant "detected unusual activity within its network."[18]

56. On or about that same time, several of Defendant's employees received emails from cybercriminal saying that they had the employees' data from Bradford.

57. Defendant determined that the threat actor infiltrated Defendant's computer systems through the account of a recently hired Bradford employee's account, which was not configured to require dual factor authentication.

58. Despite a company policy requiring dual factor authentication for employee accounts, Defendant failed to enable dual factor authentication on the new employee's account or to confirm that dual factor authentication was activated on the new employee's account.

59. Hunters International, the cybercriminal group that claims to have infiltrated Bradford's computer systems and compromised Plaintiffs' and Class Members' Private Information, locked Defendant out of its Electronic Medical

[18] *See* https://bradfordhealth.com/notice-of-data-security-incident/

Record ("EMR") system and other systems, and began several months of negotiations with Defendant, seeking a $5 million ransom to restore Defendant's access to its EMR system and other systems.

60. Once Hunters International locked Defendant out of its EMR system and other systems, the threat actor was able to go through Defendant's systems unchallenged and unobstructed, taking any and all data it came across.

61. The threat actor sent copies of patient files and employee files to Defendant to demonstrate that they had access to Defendant's EMR system and other systems.

62. Defendant was completely locked out of its EMR system and other systems for 2-3 months.

63. During the lockout, Defendant hid the Data Breach from its employees, telling them only that Defendant's servers were down, but not why.

64. During the lockout, and for more than a year afterwards, Defendant hid the Data Breach from its current and former patients, despite knowing that those patients' Private Information was compromised in the Data Breach.

65. During the lockout, Defendant's executives and owners discussed potential stories that they could tell patients and employees to cover up why Defendant's systems were down.

66. The stories proposed to cover up the Data Breach included telling patients and employees that Defendant's servers were struck by lightning. Many other options were discussed. None of those options was telling patients and employees the truth – that Defendant's systems were down because of the Data Breach.

67. The data compromised and exfiltrated during the Data Breach includes at least "individuals' names, driver's license numbers, dates of birth, medical information (including diagnosis and treatment information, physician names, and Medical Record numbers), health insurance information, financial account numbers, passport numbers, payment card numbers plus a means of access to the account, and/or Social Security numbers,"[19] and may include additional types of information Defendant has not yet disclosed.

68. Given the intentional and criminal nature of the cybersecurity attack, Plaintiffs' and Class Members' Private Information is now for sale to criminals on the dark web; meaning unauthorized parties have accessed and viewed Plaintiffs' and Class Members' Private Information.

[19] *Id*.

The Healthcare Sector Is Particularly Susceptible to Cyberattacks

69. Defendant was or should have been on notice that the Federal Bureau of Investigation ("FBI") has been concerned about data security in the healthcare sector. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "'[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII).'"[20]

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

> 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 cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[21]

[20] Jim Finkle, *FBI warns healthcare firms that they are targeted by hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[21] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (emphasis omitted).

71. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[22] In 2022, 1,802 data compromises were reported that impacted over 422 million victims—marking a 42% increase in the number of victims impacted since 2021.[23] That upward trend continues.

72. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[24] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[25] Almost 50% of the victims lost their healthcare coverage as a result of the incident, while nearly

[22] Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout, CISION PR NEWSWIRE (Jan. 19, 2017), https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html.

[23] 2022 Annual Data Breach Report, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited March 29, 2024).

[24] 2018 End-of-Year Data Breach Report, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINALWEB-V2-2.pdf (last visited March 29, 2024).

[25] 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/.

thirty percent said their insurance premiums went up after the event. Forty percent of the customers 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.[26]

73. In an article published on October 31, 2023, the HHS noted that "[r]ansomware and hacking are the primary cyber-threats in healthcare." According to HHS statistics, since 2019 there has been a 239% increase in large breaches reported to HHS' Office for Civil Rights and a 278% increase in ransomware attacks.[27]

74. Healthcare related data breaches also come at a cost to the breached entities. According to IBM's 2023 Cost of a Data Breach Report, the healthcare sector reported the highest data breach costs for the thirteenth year in a row in 2023—increasing 8.2% from $10.10 million in 2022 to $10.93 million in 2023.[28] This cost should only further incentivize service providers to both invest in and implement reasonable and adequate security measures in order to avoid financial repercussions in the event of a breach.

---

[26] *Id.*

[27] HHS' Office for Civil Rights, *HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation* (October 31, 2023) https://www.hhs.gov/about/news/2023/10/31/hhs-office-civilrights-settles-ransomware-cyber-attackinvestigation.html (last visited March 29, 2024).

[28] *Cost of a Data Breach Report 2023*, IBM, *available at* https://www.ibm.com/reports/data-breach.

75. Healthcare related data breaches have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82% of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[29]

> Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information (PII) for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.[30]

76. "[E]ven relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[31]

---

[29] *2019 HIMSS Cybersecurity Survey*, HIMSS, https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited March 29, 2024).

[30] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, CHIEF HEALTHCARE EXEC. (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

[31] The HIPAA Journal, *Editorial: Why Do Criminals Target Medical Records* (October 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited March 29, 2024).

77. Defendant knew or reasonably should have known the importance of implementing reasonable and adequate practices and procedures in order to safeguard the PII and PHI entrusted to it by individuals receiving healthcare services.

78. Defendant knew, or reasonably should have known, the importance of safeguarding the Private Information entrusted to it, and of the foreseeable consequences if Defendant's data security systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

The Data Breach was Preventable

79. Defendant's cybersecurity practices and policies were inadequate and fell short of the industry-standard measures that should have been implemented long before the Data Breach occurred. This is especially true given that the healthcare industry is frequently one of the most targeted sectors for cyberattacks. Attacks using stolen credentials have increased precipitously over the last several years.

80. Healthcare providers like Defendant are prime targets because of the information they collect and store, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and

personal information of employees and patients—all extremely valuable on underground markets.

81. This was known and obvious to Defendant as Defendant observed frequent public announcements of data breaches affecting healthcare providers and knew that information of the type Defendant collected, maintained, and stored is highly coveted and a frequent target of hackers.

82. It is well known that use of stolen credentials has long been the most popular and effective method of gaining authorized access to a company's internal networks and that companies should activate defenses to prevent such attacks.

83. According to the Federal Bureau of Investigation (FBI), phishing schemes designed to induce individuals to reveal personal information, such as network passwords, were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[32] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[33]

---

[32] *2020 Internet Crime Report*, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Mar. 29, 2024).

[33] *2021 DBIR Master's Guide*, VERIZON, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited Mar. 29, 2024).

84. The risk is so prevalent for healthcare providers that on October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[34] The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (HHS), and the FBI issued the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[35]

85. There are two primary ways to mitigate the risk of stolen credentials: user education and technical security barriers.

86. User education is the process of making employees or other users of a network aware of common disclosure schemes and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients.

87. Companies can also greatly reduce the flow of fraudulent e-mails by installing technical security barriers including software that scans all incoming

[34] *Ransomware Activity Targeting the Healthcare and Public Health Sector*, JOINT CYBERSECURITY ADVISORY, https://www.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited Mar. 28, 2024).

[35] *Id*.

messages for harmful attachments or malicious content and implementing certain security measures governing e-mail transmissions, including Sender Policy Framework (SPF) (e-mail authentication method used to prevent spammers from sending messages on behalf of a company's domain), DomainKeys Identified Mail (DKIM) (e-mail authentication method used to ensure messages are not altered in transit between the sending and recipient servers), and Domain-based Message Authentication, Reporting and Conformance (DMARC), which "builds on the widely deployed [SPF] and [DKIM] protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email."[36]

88. In addition to mitigating the risk of stolen credentials, the CISA guidance encourages organizations to prevent unauthorized access by:

- Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;
- Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;

[36] *#StopRansomware Guide*, https://www.cisa.gov/stopransomware/ransomware-guide (last visited March 28, 2024).

- Ensuring devices are properly configured and that security features are enabled;
- Employing best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and
- Disabling operating system network file sharing protocol known as Server Message Block (SMB) which is used by threat actors to travel through a network to spread malware or access sensitive data.[37]

89. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[38]

90. Despite holding the Private Information of millions of patients, Defendant failed to adhere these recommended best practices. Indeed, had Defendant implemented common sense security measures, the hackers never could have accessed millions of patient and employee files and the breach would have

[37] *Id*.

[38] *Id*.

been prevented or much smaller in scope. Defendant also lacked the necessary safeguards to detect and prevent attacks and failed to implement adequate monitoring or control systems to detect the unauthorized infiltration after it occurred.

91. Defendant, like any entity in the healthcare industry storing valuable and sensitive data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of patient files. Defendant's procedures and policies were below industry-standards and are inexcusable given Defendant's knowledge that it was a prime target for cyberattacks.

Allegations Relating to Plaintiff F.P.

92. Plaintiff F.P. is a resident and citizen of Birmingham, Alabama. He received treatment at Bradford from September 20, 2021 to December 23, 2021. Following his initial three-month treatment period, Plaintiff F.P. returned to Bradford for monthly check-ins over a six-month period beginning in February of 2022.

93. For purposes of receiving medical treatment, Plaintiff F.P. was required to provide Defendant with his sensitive PII and PHI, including, among other information, his full name, addresses, driver's license number, dates of birth, medical information (including diagnosis and treatment information, physician

names, and Medical Record numbers), health insurance information, financial account numbers, credit or payment card information, Social Security number, and information regarding Plaintiff F.P.'s children, parents, and siblings.

94. Plaintiff F.P. first learned of the Data Breach upon receiving Bradford's written notice dated May 30, 2025. Notably, Bradford mailed the notice to Plaintiff F.P.'s former address, despite having been informed of his current address on multiple occasions.

95. As a result of the Data Breach, Plaintiff F.P. has suffered lost time, annoyance, interference, and inconvenience addressing and monitoring for adverse personal impacts caused by the Data Breach. This is time Plaintiff F.P. otherwise would have spent performing other activities.

96. In addition, Plaintiff F.P. has suffered and will continue to suffer emotional distress as a result of the Data Breach, and has increased concerns for the loss of his privacy and the release of his Private Information, which he would not have suffered had Defendant implemented the necessary and proper safeguards to protect Plaintiffs' and Class Members' Private Information from theft.

97. The Private Information that was accessed in the Data Breach was the kind of sensitive information that can be used to commit fraud, including medical fraud, and identity theft. It was reasonable and foreseeable that Plaintiff F.P. would take, and continue to take, necessary measures to protect his Private Information.

98. Plaintiff F.P. reasonably believes– based on public reports and the severity of the Data Breach– that Defendant did not maintain and continue to not maintain his Private Information with adequate protections and safeguards and that his Private Information was part of the massive amount of Private Information exposed during the Data Breach.

99. Plaintiff F.P. has a continuing interest in ensuring that his Private Information, which, upon information and belief, remain in Defendant's possession, is protected and safeguarded from further and future breaches.

100. Plaintiff F.P. suffered actual injury in the form of damages to and loss of value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving healthcare services, which was compromised in, and as a result of, the Data Breach.

101. As a result of the Data Breach, Plaintiff F.P. will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

Allegations Relating to Plaintiff C.W.

102. Plaintiff C.W. is a resident and citizen of Florida and was an inpatient client of Bradford in 2022 and 2023..

103. For purposes of receiving medical treatment, Plaintiff C.W. was required to provide Defendant with his sensitive PII and PHI, including, among

other information, his full name, addresses, driver's license number, dates of birth, medical information (including diagnosis and treatment information, physician names, and Medical Record numbers), health insurance information, financial account numbers, credit or payment card information, and Social Security number.

104. Plaintiff C.W. learned of the Data Breach for the first time upon receiving the notification mailed by Bradford.

105. From the time of the Data Breach to the present, Plaintiff C.W. has been a victim of identity theft, financial fraud, seen an uptick in unwanted spam emails, and suffered other harms which Plaintiff C.W. reasonably believes occurred as a result of the Data Breach. As one example, an unauthorized credit card account was opened in Plaintiff C.W.'s name with Chase Bank. Plaintiff C.W. did not authorize the opening of this account, and does not believe the charges made on this account are legitimate. Approximately $3,500 was charged to the unauthorized Chase account. Plaintiff C.W. has challenged the charges as unauthorized. Chase Bank rejected the challenge and has sent the account to collections, which has harmed Plaintiff C.W.'s credit score.

106. As a result of the Data Breach, Plaintiff C.W. has also suffered lost time, annoyance, interference, and inconvenience addressing and monitoring for adverse personal impacts caused by the Data Breach, including addressing identity theft and financial fraud such as the unauthorized account opened in his name at

Chase. This is time Plaintiff C.W. otherwise would have spent performing other activities.

107. In addition, C.W. has suffered and will continue to suffer emotional distress as a result of the Data Breach, and has increased concerns for the loss of his privacy and the release of his Private Information, which he would not have suffered had Defendant implemented the necessary and proper safeguards to protect Plaintiffs' and Class Members' Private Information from theft.

108. The Private Information that was accessed in the Data Breach was the kind of sensitive information that can be used to commit fraud, including medical fraud, and identity theft. It was reasonable and foreseeable that Plaintiff C.W. would take, and continue to take, necessary measures to protect his Private Information.

109. Plaintiff C.W. reasonably believes– based on public reports and the severity of the Data Breach– that Defendant did not maintain and continue to not maintain his Private Information with adequate protections and safeguards and that his Private Information was part of the massive amount of Private Information exposed during the Data Breach.

110. Plaintiff C.W. has a continuing interest in ensuring that his Private Information, which, upon information and belief, remain in Defendant's possession, is protected and safeguarded from further and future breaches.

111. Plaintiff C.W. suffered actual injury in the form of damages to and loss of value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving healthcare services, which was compromised in, and as a result, of the Data Breach.

112. As a result of the Data Breach, Plaintiff C.W. will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

The Value of Private Information and the Effects of Unauthorized Disclosure

113. At all relevant times, Defendant was well aware that the Private Information it collects from Plaintiffs and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

114. The value of Private Information is axiomatic considering the value of "big data" in corporate America.

115. Private Information is also a valuable commodity to cyber attackers. The U.S. Attorney General confirmed in 2020 that "hackers" target consumers' sensitive personal information because it "has economic value."[39]

[39] *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice (February 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited March 29, 2024).

116. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use Private Information to commit an array of crimes including identify theft, and medical and financial fraud.[40] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground websites, commonly referred to as the dark web.

117. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363.[41]

118. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

119. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "'Medical identity theft is a growing and dangerous crime that

[40] *What to Know About Identify Theft*, Fed. Trade Comm'n, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited March 29, 2024).

[41] *Data Breaches: In the Healthcare Sector,* Ctr. for Internet Sec., https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited March 29, 2024).

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.'"[42]

120. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.[43]

121. The ramifications of Defendant's failures to keep Plaintiffs' and Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for 6 to 12 months or even longer.

122. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen

[42] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

[43] *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIV. (Apr. 8, 2014), https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf.

Private Information on the internet, thereby making such information publicly available.

123. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[44] This gives thieves ample time to seek multiple treatments under the victim's name. And 40% of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[45]

124. As a company operating in the health sector, Defendant knew, or reasonably should have known, the importance of safeguarding Plaintiffs' and Class Members' Private Information entrusted to it, and of the foreseeable consequences if Defendant's data security systems were breached. This includes the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

[44] *See Medical ID Theft Checklist*, IdentityForce https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited March 29, 2024).

[45] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), Experian (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

Defendant Failed to Comply with Federal Law and Regulatory Guidance

125. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components. [46]

126. Defendant is a covered entity under HIPAA and is therefore 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.

127. These rules establish national standards for the protection of patient information, including PHI, 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. 45 C.F.R. § 160.103.

[46] *What is Considered Protected Health Information Under HIPAA?*, HIPAA J. (Jan. 1, 2023), https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.

128. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[47]

129. HIPAA requires that Defendant implement appropriate safeguards for this information.[48]

130. Title II of HIPAA contains the Administrative Simplification provisions. 42 U.S.C. §§1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant failed to safeguard. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

131. HIPAA requires that Defendant provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—i.e. non-encrypted data.[49]

132. The HIPAA Breach Notification Rule, 45 CFR §§164.400-414, also required Defendant to provide notice of the breach to each affected individual

[47] 45 C.F.R. § 164.502.

[48] 45 C.F.R. § 164.530(c)(1).

[49] 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

"without unreasonable delay and in no case later than 60 days following discovery of a breach."[50]

133. Based on information and belief, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. Defendant's security failures include, but are not limited to:

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

b. Failing to adequately protect the PHI of patients;

c. Failing to ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

[50] *Breach Notification Rule*, U.S. Dep't of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited March 29, 2024) (emphasis added).

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

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

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

h. Failing to ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4);

i. Failing to train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b);

j. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

k. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2); and/or

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

Defendant Failed to Comply with FTC Guidelines

134. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[51]

135. Defendant was prohibited by the Federal Trade Commission Act ("FTCA") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to

[51] *Start with Security*, FTC, https://www.ftc.gov/system/files/documents/plain- language/pdf0205-startwithsecurity.pdf (last visited Mar. 29, 2024).

maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA.[52]

136. According to the FTC, the need for data security should be factored into all business decision-making.[53]

137. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[54] The guidelines note that 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.

138. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and

---

[52] *See, e.g.*, *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020) (citing *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)).

[53] *Start With Security: A Guide for Business*, Fed. Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 29, 2024).

[54] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 29, 2024).

verify that third-party service providers have implemented reasonable security measures.[55] This is consistent with guidance provided by the FBI, HHS, and the principles set forth in the CISA 2020 guidance.

139. The FTC also states that outdated software undermines security, and recommends that software be updated regularly, third party patches be implemented as they are issued, and automated tools should be used to track which version of software is running and whether updates are available.[56]

140. The FTC strongly encourages businesses to "[p]ut procedures in place to keep your security current and address vulnerabilities that may arise," including to "[c]heck expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems." The FTC also cautions businesses to heed credible security warnings and move quickly to fix them. Businesses are strongly encouraged to "[h]ave an effective process in place to receive and address security vulnerability reports." [57]

---

[55] *Start With Security: A Guide for Business*, Fed. Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 29, 2024).

[56] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 29, 2024).

[57] *Id*.

141. 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 FTCA, 15 U.S.C. §45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[58]

142. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. §45.

143. Defendant was fully aware of its obligations to protect the Private Information of Plaintiffs and Class Members because of Defendant's position healthcare provider whose business includes the collection, storage, and safeguarding of PII and PHI. Defendant was also aware of the significant repercussions that would result from Defendant's failure to make good on those obligations.

[58] *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Mar. 29, 2024).

144. Defendant was fully aware of its obligation to implement and use reasonable measures to protect the PHI of the patients but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring.

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

Cybercriminals Have and Will Continue to Use Plaintiffs' and Class Members' PII and PHI for Nefarious Purposes

146. Plaintiffs' and Class Members' highly sensitive PII and PHI is of great value to cybercriminals, and the data stolen in the Data Breach can be used in a variety of ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune and stolen information. The cybercriminals' motives for the Data Breach were purely nefarious and malicious in nature: their one goal was to access systems, including Defendant's systems, in order to obtain valuable PII and PHI to sell on the dark web.

147. Every year, identity theft causes tens of billions of dollars of losses to victims in the United States.[59] For example, with the PII stolen in the Data Breach,

[59] *Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited March 29, 2024) (discussing Javelin Strategy & Research's report *2018 Identity Fraud: Fraud Enters a New Era of Complexity*).

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.[60] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

148. PII 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.

149. These risks are both certainly impending and substantial. As the FTC has reported, if cyber attackers get access to PII, they will use it.[61]

150. Cyber attackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

---

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

[61] 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.

151. [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[62]

152. If cyber criminals manage to access PII, health insurance information, and other personally sensitive data, as is the case with this Data Breach, there is no limit to the amount of fraud to which Defendant may have exposed Plaintiffs and Class Members.

Defendant Owed a Duty to Plaintiffs and Class Members to Keep Their Private Information Secure and Protect It From Being Compromised, Lost, Stolen, Accessed, or Misused

153. In addition to its obligations under state laws and regulations, Defendant owed a common law duty to Plaintiffs and Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties. This duty extends to Defendant's

[62] Stolen Laptops Lead to Important HIPAA Settlements, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Apr. 22, 2014), https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

obligations to safeguard PII and PHI shared with subcontractors and service vendors who received Private Information from Defendant, and to conduct ongoing, robust due diligence into such subcontractors and service vendors prior to contracting and throughout any relationship.

154. Defendant further owed and breached its duties to Plaintiffs and Class Members to implement processes and specifications that would detect a breach of Defendant's security systems in a timely manner and to timely act upon warnings and alerts, including those generated by Defendant's own security systems.

155. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, cyber attackers were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiffs' and Class Members' Private Information as detailed above, and Plaintiffs are now at a heightened risk of identity theft and fraud.

156. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiffs' and Class Members' Private Information 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 Plaintiffs' and Class

Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

157. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite Defendant's obligation to protect patient data.

158. Had Defendant remedied the deficiencies in Defendant's data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into Defendant's systems and, ultimately, the theft of Plaintiffs' and Class Members' Private Information.

The Impact of the Data Breach on Victims

159. The Private Information exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit identity fraud, including medical-related identity theft and fraud, one of the most dangerous and costly forms of identity theft.

160. According to a *Reuters* investigation that included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts, medical data for sale on underground markets "includes names, birth dates, policy numbers, diagnosis codes and billing information" which fraudsters commonly use "to create fake IDs to buy medical equipment or drugs that can be

resold, or they combine a patient number with a false provider number and file made-up claims with insurers."[63]

161. According to Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, "Health information is a treasure trove for criminals [because] by compromising it, by stealing it, by having it sold, you have seven to 10 personal identifying characteristics of an individual."[64] For this reason, a patient's full medical records can sell for up to $1,000 on the dark web, while credit card numbers and Social Security numbers may cost $5 or less.[65]

162. As noted by Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies: "The reason for this price discrepancy—like any other good or service—is perceived value. While a credit card number is easily canceled, medical records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information. Once

[63] Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS (Sep. 24, 2014), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-recordis-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

[64] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon

[65] . Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your- personalinformation-is-selling-for-on-the-dark-web/.

records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient's identity to open credit cards and fraudulent loans."[66]

163. Indeed, while federal law generally limits an individual's responsibility for fraudulent charges on a credit card to $50, there are no such protections for a stolen medical identity. According to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of $13,500 in out-of-pocket costs to resolve the crime.[67] Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and Medicaid benefits (52%). Only 14% of respondents said that the identity thieves used the information to obtain fraudulent credit accounts, indicating that medical information is a much more profitable market.[68]

---

[66] Paul Nadrag, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, FIERCE HEALTHCARE (Jan. 26, 2021, 3:55 PM), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medicalrecords-are-hottest-items-dark-web.

[67] *Fifth Annual Study on Medical Identity Theft*, PONEMON INSTITUTE (Feb. 2015), https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 ("Ponemon Study").

[68] *Id*. at 9.

164. According to the Ponemon study, "[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate."[69]

165. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with 19% responding that they missed out on employment opportunities as a result.[70]

166. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because HIPAA regulations require the victim to be personally involved in the resolution of the crime.[71] In some cases, victims may not even be able to access medical records using their personal information because they include a false name or data points taken from another person's records. Consequently, only 10% of medical identity theft victims

[69] *Id*. at 2.

[70] *Id*. at 14.

[71] *Id*. at 1.

responded that they "achieve[d] a completely satisfactory conclusion of the incident."[72]

167. Moreover, it can take months or years for victims to even discover they are the victim of medical-related identity theft or fraud given the difficulties associated with accessing medical records and healthcare statements. For example, the FTC notes that victims may only discover their identity has been compromised after they:

- Receive a bill for medical services they did not receive;
- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;
- Find erroneous listings of office visits or treatments on their explanation of benefits (EOB);
- Receive information from their health plan that they have reached their limit on benefits; or
- Be denied insurance because their medical records show a condition they do not have.[73]

[72] *Id*.

[73] *Medical Identity Theft, FAQs for Health Care Providers and Health Plans*, FTC.GOV, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faqhealth-care-health-plan.pdf (last visited Mar. 29, 2024).

168. Perhaps most dangerous, however, is the potential for misdiagnoses or treatment. According to Ann Patterson, a senior vice president of the Medical Identity Fraud Alliance, "About 20 percent of victims have told us that they got the wrong diagnosis or treatment, or that their care was delayed because there was confusion about what was true in their records due to the identity theft." [74] This echoes the Ponemon study, which notes that "many respondents are at risk for further theft or errors in healthcare records that could jeopardize medical treatments and diagnosis."[75]

169. According to a Consumer Reports article entitled *The Rise of Medical Identity Theft*, this outcome "isn't a hypothetical problem" as the "long tail on medical identity theft can create havoc in victims' lives."[76] As one example, a pregnant woman reportedly used a victim's medical identity to pay for maternity care at a nearby hospital. When the infant was born with drugs in her system, the state threatened to take the *victim's* four children away—not realizing her identity had been stolen. The victim ultimately had to submit to a DNA test to remove her

[74] Michelle Andrews, *The Rise of Medical Identity Theft*, CONSUMER REPORTS, https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited Mar. 29, 2024).

[75] Ponemon Study at 1.

[76] Michelle Andrews, *The Rise of Medical Identity Theft*, CONSUMER REPORTS, https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited Mar. 29, 2024).

name from the infant's birth certificate, but it took years to get her medical records corrected.[77]

170. Other types of medical fraud include "leveraging details specific to a disease or terminal illness, and long-term identity theft."[78] According to Tom Kellermann, "Traditional criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[79] Long-term identity theft occurs when fraudsters combine a victim's data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

171. Many victims of the Data Breach have likely already experienced significant harms as the result of the Data Breach, including, but not limited to, medical-related identity theft and fraud. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and healthcare

[77] *Id*.

[78] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[79] *Id*.

statements, checking credit reports, and spending time and effort searching for unauthorized activity.

172. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fear for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.[80]

173. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;

[80] *Identity Theft: The Aftermath 2017*, ITRC, https://www.idtheftcenter.org/wpcontent/uploads/images/page-docs/Aftermath_2017.pdf (last visited March 29, 2024).

- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[81]

174. The unauthorized disclosure of the sensitive PHI and other Private Information to data thieves also deprives its owner of its value, which has been recognized by courts as an independent form of harm.[82]

175. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach

[81] *Id.*

[82] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

176. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. the unconsented disclosure of confidential information to a third party;

b. losing the value of the explicit and implicit promises of data security;

c. identity theft and fraud resulting from the theft of their Private Information;

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

e. anxiety, emotional distress, and loss of privacy;

f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts,

including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

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 mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their Private Information being in the possession of one or many unauthorized third parties.

177. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

178. 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 "[r]esolving the problems caused by identity theft [could] take more than a year for some victims."[83]

179. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes. According to the Government Accountability Office, which conducted a study regarding data breaches: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[84]

180. Plaintiffs and Class Members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or

[83] Erika Harrell, & Lynn Langton, *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUST., OFF. OF JUST. PROGRAMS BUREAU OF JUST. STATS. (Dec. 2013), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

[84] PERSONAL INFORMATION: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown, GAO, http://www.gao.gov/new.items/d07737.pdf (last visited Mar. 29, 2024).

important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[85]

181. Because of the value consumers place on data privacy and security, healthcare providers with robust data security practices are viewed more favorably by patients and can command higher prices than those who do not. Consequently, had patients known the truth about Defendant's data security practices—that it did not adequately protect and store their Private Information, including PHI—they would not have sought medical care and/or filled prescriptions practices affiliated with Defendant or would have paid significantly less. As such, Plaintiffs and Class Members did not receive the benefit of their bargain with Defendant because they paid for the value of services they did not receive.

182. Plaintiffs and Class Members have a direct interest in Defendant's promises and duties to protect their Private Information, *i.e.*, that Defendant *not increase* their risk of identity theft and fraud. Because Defendant failed to live up to its promises and duties in this respect, Plaintiffs and Class Members seek the

[85] *BEYOND THE BOTTOM LINE: THE REAL COST OF DATA BREACHES*, FIREEYE, https://www2.fireeye.com/rs/848-DID-242/images/rpt-beyond-bottomline.pdf (last visited Mar. 29, 2024).

present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Defendant's wrongful conduct. Through this remedy, Plaintiffs and Class Members seek to restore themselves and class members as close to the same position as they would have occupied but for Defendant's wrongful conduct, namely Defendant's failure to adequately protect Plaintiffs' and Class Members' Private Information.

183. Plaintiffs and Class Members further seek to recover the value of the unauthorized access to their Private Information permitted through Defendant's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's Private Information is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiffs and Class

Members have a protectible property interest in their Private Information; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

184. Because Defendant continues to hold the Private Information of patients, Plaintiffs and Class Members have an undeniable interest in ensuring that their Private Information is secured, remains secure, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

185. Plaintiffs bring this class action on behalf of themselves and all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure.

186. The Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose personal health information was compromised in the Data Breach announced by Addiction and Mental Health Services, LLC d/b/a Bradford Health Services on May 30, 2025.

187. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, current or former employees, 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; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

188. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

189. Numerosity, Fed. R. Civ. P. 23(a)(1): The members of the Class are so numerous that joinder of all of them is impracticable. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Defendant, upon information and belief, hundreds of thousands of individuals were impacted. The Class is apparently identifiable within Defendant's records.

190. Commonality and Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These common questions of law and fact are such that there is a well-defined community of interest in this litigation. The common questions of law and fact include, without limitation:

a. Whether Defendant owed Plaintiffs and Class Members a duty to implement and maintain reasonable security procedures and practices to protect their Private Information;

b. Whether Defendant violated its duty to implement reasonable security systems to protect Plaintiffs' and Class Members' Private Information;

c. Whether Defendant's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class Members;

d. Whether Defendant owed a duty to Plaintiffs and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Private Information;

e. Whether Defendant violated its duty to exercise due care in collecting, storing, safeguarding, and/or obtaining their Private Information;

f. Whether Defendant's breach of its duty to exercise due care in collecting, storing, safeguarding, and/or obtaining their Private Information directly and/or proximately caused damages to Plaintiffs and Class Members;

g. Whether Defendant breached its contractual obligations to Plaintiffs and Class Members;

h. Whether Defendant received a benefit without proper restitution making it unjust for Defendant to retain the benefit without commensurate compensation;

i. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class Members' Private Information;

j. Whether Defendant adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

k. Whether Defendant and class members are entitled to damages to pay for future protective measures like credit monitoring and monitoring for misuse of medical information; and

l. Whether class members are entitled to statutory damages, compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

191. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of the claims of the members of the Class because all class members had their Private Information compromised in the Data Breach and were harmed as a result.

192. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has 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 and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect the Class 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 Plaintiff.

193. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no known interest antagonistic to those of the Class and their interests are aligned with Class members' interests. Plaintiffs were subject to the same Data Breach as class members, suffered similar harms, and face similar threats due to the Data Breach. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions, including data breach cases involving multiple classes and data breach claims.

194. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The 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 hundreds 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.

195. The nature of this action and the nature of laws available to Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of the Class 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.

196. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

198. Unless a Class-wide injunction is issued, Plaintiffs and Class Members remain at risk that Defendant will continue to fail to properly secure the Private Information of Plaintiffs and Class Members resulting in another data breach, continue to refuse to provide proper notification to Class Members regarding the Data Breach, and continue to act unlawfully as set forth in this Class Action Complaint.

199. Defendant acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

200. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

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

- Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- Whether Defendant failed to implement and maintain reasonable and adequate security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- Whether Class Members are entitled to actual damages, additional credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct; and
- Whether Class Members are entitled to statutory damages as a result of Defendant's wrongful conduct.

201. Class Identity: The members of the Class are readily identifiable and ascertainable. Defendant and/or its affiliates, among others, possess the information to identify and contact class members.

CLAIMS FOR RELIEF

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

202. Plaintiffs repeat and reallege every allegation set forth in Paragraphs 1 through 201 as though fully set forth herein.

203. Plaintiffs and Class Members were required to submit their Private Information to Defendant as a condition of receiving healthcare services.

204. Defendant stored Plaintiffs' and Class Members' Private Information for purposes of providing healthcare services as well as for commercial gain.

205. Defendant knew, or should have known, of the risks inherent in collecting and storing the Private Information of Plaintiffs and Class Members.

206. As described above, Defendant owed duties of care to Plaintiffs and Class Members whose Private Information had been entrusted with Defendant.

207. The duties of care owed by Defendant include a duty to exercise reasonable care in protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure or access. Defendant acknowledged this duty in its privacy policies, where Defendant promised not to disclose PHI and other Private Information without authorization and to abide by all federal laws and regulations.

208. The duties of care owed by Defendant include also include a duty to provide adequate data security, consistent with industry standards, to ensure that

Defendant's systems and networks adequately protected Plaintiffs' and Class Members' Private Information.

209. Under HIPAA, Defendant had a special relationship with Plaintiffs and Class Members who entrusted Defendant to adequately safeguard their confidential personal, financial, and medical information.

210. Defendant also entered into a special relationship with Plaintiffs and Class Members because Defendant collected the Private Information of Plaintiffs and Class Members – information that Plaintiffs and Class Members were required to provide in order to receive medical services, prescriptions, and payment for healthcare services.

211. Defendant's duty to use reasonable care in protecting Plaintiffs' and Class Members' Private Information arises as a result of the parties' relationship, as well as common law and federal law, including the HIPAA regulations described above and Defendant's own policies and promises regarding privacy and data security.

212. Defendant breached its duty to Plaintiffs and Class Members in numerous ways, as described herein, including by:

- Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Private Information of Plaintiffs and Class Members;

- Failing to comply with industry standard data security measures for the healthcare industry leading up to the Data Breach;
- Failing to comply with its own privacy policies;
- Failing to comply with regulations protecting the Private Information at issue during the period of the Data Breach;
- Failing to adequately monitor, evaluate, and ensure the security of Defendant's network and systems; and
- Failing to recognize in a timely manner that Private Information had been compromised.

213. Defendant acted with wanton disregard for the security of Plaintiffs' and Class Members' Private Information. Defendant knew or reasonably should have known that it had inadequate data security practices to safeguard such information, and Defendant knew or should have known that data thieves were attempting to access databases containing Private Information such as that entrusted to Defendant.

214. Plaintiffs' and Class Members' Private Information would not have been compromised but for Defendant's wrongful and negligent breach of its duties.

215. But for Defendant's wrongful and negligent breaches of the duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

216. Defendant's failure to take proper security measures to protect the sensitive PHI and other Private Information of Plaintiffs and Class Members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and copying of Private Information by unauthorized third parties. Given that healthcare providers and affiliates are prime targets for hackers, Plaintiffs and Class Members are part of a foreseeable, discernible group that was at high risk of having their Private Information misused or disclosed if not adequately protected by Defendant.

217. It was also foreseeable that Defendant's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiffs and Class Members.

218. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have and will suffer damages in an amount to be proven at trial, including: (i) the loss of rental or use value of their Private Information; (ii) the unconsented disclosure of their Private Information to unauthorized third parties; (iii) out-of- pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with 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 fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it; (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 Private Information for the rest of their lives; and (ix) any nominal damages that may be awarded.

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

219. Plaintiffs repeat and reallege every allegation set forth in Paragraphs 1 through 201 as though fully set forth herein.

220. The Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC.

221. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate data security practices to safeguard Plaintiffs' and Class Members' Private Information.

222. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

223. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

224. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

225. Pursuant to HIPAA (42 U.S.C. §§ 1302d, *et seq*.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

226. Plaintiffs and Class Members are within the class of persons that HIPAA and its implementing regulations were intended to protect.

227. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

228. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act (15 U.S.C. § 45) and HIPAA (42 U.S.C. §§ 1302d, *et seq*.), by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiffs' and Class Members' Private Information.

229. Defendant's conduct was unreasonable given the nature and amount of Private Information Defendant obtained, stored, and disseminated in the regular course of its business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiffs and Class Members.

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

231. But for Defendant's wrongful and negligent breaches of its duties owed to Plaintiffs and Class Members. Plaintiffs and Class Members would not have been injured.

232. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties to Plaintiffs and Class Members. Defendant knew or reasonably should have known that it was failing to meet its duties, and that Defendant's breaches of those duties would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

233. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have injury and sustained actual losses and damages as alleged herein, in an amount to be proven at trial. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT III
Breach of Contract
(On Behalf of Plaintiffs and the Class)

234. Plaintiffs repeat and reallege every allegation set forth in Paragraphs 1 through 201 as though fully set forth herein.

235. Defendant's Notice of Privacy Practices is an agreement between Defendant and the individuals who provided their PII and PHI to Defendant, including Plaintiffs and Class Members.

236. The Notice of Privacy Policy applies to all of the "Protected Health Information and records" Plaintiffs and Class Members provided to Defendant. [86]

237. At all relevant times, including through the date of the Data Breach and through the present, Defendant's Notice of Privacy Policy included the promise that Defendant would "maintain the privacy and security of your Protected Health Information and records."[87]

238. At all relevant times, including through the date of the Data Breach and through the present, Defendant's Notice of Privacy Policy included the promise that Defendant would "notify you if there is a breach of your unsecured Protected Health Information or unsecured records."[88]

---

[86] *See* https://bradfordhealth.com/notice-of-privacy-practices

[87] *Id*.

[88] *Id*.

239. At all relevant times, including through the date of the Data Breach and through the present, Defendant's Notice of Privacy Policy included the promise that Defendant would only disclose the "Protected Health Information and records" in its possession "when you provide your written authorization/consent on a written or electronic form."[89]

240. Plaintiffs and Class Members did not provide their written authorization/consent for Defendant to share their Private Information with criminal hackers.

241. Plaintiffs and Class Members on the one side and Defendant on the other side formed a contract when Plaintiffs and Class Members provided Private Information to Defendant subject to its Notice of Privacy Policy.

242. Plaintiffs and Class Members fully performed their obligations under their contracts with Defendant.

243. Defendant breached its agreement with Plaintiffs and Class Members by failing to protect their Private Information, including their the "Protected Health Information and records." Specifically, Defendant (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

[89] *Id*.

244. Defendant knew that a breach of these contracts would harm Plaintiffs and Class Members.

245. Defendant breached these contracts while acting in the ordinary course of business by failing to utilize adequate data security practices to safeguard Plaintiffs' and Class Members' Private Information, and by otherwise not protecting Plaintiffs' and Class Members' Private Information, as stated herein.

246. Plaintiffs and Class Members were harmed by Defendant's breaches in failing to use reasonable data security measures to safely maintain and protect Plaintiffs' and Class Members' Private Information.

247. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, medical fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, medical fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports,

among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT IV
Breach of Implied Contract
Pleaded in the Alternative to Breach of Express Contract
(On Behalf of Plaintiffs and the Class)

248. Plaintiffs repeat and reallege every allegation set forth in Paragraphs 1 through 201 as though fully set forth herein.

249. This Count is pleaded in the alternative to the breach of contract claim (Count III) above.

250. Plaintiffs and Class Members entered into an implied contract with Defendant when they provided their Private Information to Defendant in connection with receiving healthcare services or employment from Defendant.

251. As part of these transactions, Defendant agreed to safeguard and protect the Private Information of Plaintiffs and Class Members and to timely and accurately notify them if their Private Information was breached or compromised.

252. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiffs and Class Members believed that Defendant, as it was legally obligated to do, would use part of the monies paid to Defendant under the implied contracts or the monies obtained from the benefits derived from the Private Information they provided to fund proper and reasonable data security practices.

253. Plaintiffs and Class Members would not have provided and entrusted their Private Information to Defendant or would have paid less for Defendant's services in the absence of the implied contract or implied terms between them and Defendant. The safeguarding of the Private Information of Plaintiffs and Class Members was critical to realize the intent of the parties.

254. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

255. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to protect their Private Information, including their the "Protected Health Information and records." Specifically, Defendant (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

256. Defendant knew that a breach of these implied contracts would harm Plaintiffs and Class Members.

257. Defendant breached these implied contracts while acting in the ordinary course of business by failing to utilize adequate data security practices to safeguard Plaintiffs' and Class Members' Private Information, and by otherwise not protecting Plaintiffs' and Class Members' Private Information, as stated herein.

258. Plaintiffs and Class Members were harmed by Defendant's breaches of the implied contracts in failing to use reasonable data security measures to safely maintain and protect Plaintiffs' and Class Members' Private Information.

259. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, medical fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, medical fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit

reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT V
Unjust Enrichment
Pleaded in the Alternative to Breach of Express Contract and Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

260. Plaintiffs repeat and reallege every allegation set forth in Paragraphs 1 through 201 as though fully set forth herein.

261. This Count is pleaded in the alternative to the breach of contract claim (Count III) and breach of implied contract (Count IV) claim above.

262. Plaintiffs and Class Members have an interest, both equitable and legal, in their Private Information that was conferred upon, collected by, and maintained by the Defendant and which was stolen in the Data Breach. This information has independent value.

263. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of payments for medical and healthcare services, including those paid indirectly by Plaintiffs and Class Members to Defendant.

264. Defendant appreciated and had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

265. The price for medical and healthcare services that Plaintiffs and Class Members paid (directly or indirectly) to Defendant should have been used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

266. Likewise, in exchange for receiving Plaintiffs' and Class Members' valuable Private Information, which Defendant was able to use for its own business purposes and which provided actual value to Defendant, Defendant was obligated to devote sufficient resources to reasonable data privacy and security practices and procedures.

267. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages as described herein.

268. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement – or adequately implement – the data privacy and security practices that Plaintiffs and Class Members paid for and that

were otherwise mandated by HIPAA regulations, federal, state, and local laws, and industry standards.

269. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds Defendant received from Plaintiffs and Class Members, including damages equaling the difference in value between medical and healthcare services that included implementation of reasonable data privacy and security practices that Plaintiffs and Class Members paid for and the services without reasonable data privacy and security practices that they actually received.

270. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendant traceable to Plaintiffs and Class Members.

COUNT VI
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

271. Plaintiffs repeat and reallege every allegation set forth in Paragraphs 1 through 201 as though fully set forth herein.

272. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

273. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further cyberattacks and data breaches that could compromise their Private Information.

274. Defendant still possesses Private Information pertaining to Plaintiffs and Class Members, which means their Private Information remains at risk of further breaches because Defendant's data security measures remain inadequate. Plaintiffs and Class Members continue to suffer injuries as a result of the compromise of their Private Information and remain at an imminent risk that additional compromises of their Private Information will occur in the future.

275. Pursuant to the Declaratory Judgment Act, Plaintiffs seek a declaration that: (a) Defendant's existing data security measures do not comply with their obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) Defendant must have policies and procedures in place to ensure the parties with whom Defendant shares sensitive personal information maintain reasonable, industry-standard security measures, including, but not limited to, those listed at (ii), (a)-(i), *infra*, and must comply with those policies and procedures; (2) Defendant must: (i) purge, delete, or destroy in a

reasonably secure manner Plaintiffs' and Class Members' Private Information if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. Engaging 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;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training Defendant's security personnel regarding any new or modified procedures;

d. Encrypting Private Information and segmenting Private Information by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of its systems;

e. Purging, deleting, and destroying in a reasonable and secure manner Private Information not necessary to perform essential business functions;

f. Conducting regular database scanning and security checks;

g. Conducting regular employee education regarding best security practices;

h. Implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and

i. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

COUNT VII

Violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-1 et seq.

(On Behalf of Plaintiffs and the Class)

276. Plaintiffs repeat and reallege every allegation set forth in Paragraphs 1 through 201 as though fully set forth herein.

277. Defendant is a "person" as defined by Ala. Code § 8-19-3(10).

278. Plaintiffs and Class Members are "consumers" as defined by Ala. Code § 8-19-3(4).

279. Defendant advertised, offered, or sold goods or services in Alabama, and engaged in trade or commerce directly or indirectly affecting the people of Alabama.

280. Defendant engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce, including acts and practices that would violate Section 5(a)(1) of the FTC Act, as interpreted by the FTC and federal courts.

281. Defendant's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' Private Information, 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 sufficiently improve security and privacy measures despite knowing the risk of 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 Plaintiffs' and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or properly secure Plaintiffs' and Subclass Members' Private Information;

g. 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 Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45; and

h. Failing to provide timely and effective notice of the Data Breach as required by Ala. Code 1975, 8-38-2.

282. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

283. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

284. Had Defendant disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, were 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.

285. Defendant was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs and Class Members.

286. Defendant accepted the responsibility of protecting Plaintiffs' and Class Members' Private Information while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Class

Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

287. Defendant acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs and Class Members' rights. Defendant's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

288. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft, medical identity theft, loss of value of their Private Information; overpayment for Defendant's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

289. Defendant's deceptive acts and practices caused substantial injury to Plaintiffs and Class Members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

290. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including, pursuant to § 8-19-10(a) the greater of (1) actual

damages or (2) statutory damages of $100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are the proper class representatives; and appoint Plaintiffs' counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and Class Members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of its unlawful acts, omissions, and practices;

F. That Plaintiffs be granted the declaratory and injunctive relief sought herein;

G. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial in the instant action.

Dated: June 11, 2025

Respectfully submitted,

/s/ _____

DiCELLO LEVITT LLP
Amy E. Keller (*pro hac vice* forthcoming)
Nada Djordjevic (*pro hac vice* forthcoming)
Ten North Dearborn St., Sixth Floor
Chicago, Illinois 60602
Tel.: (312) 214-7900
akeller@dicellolevitt.com
ndjordjevic@dicellolevitt.com

Eli Hare (ASB-1024-T20Q)
DiCELLO LEVITT LLP
505 20th Street North, Suite 1500
Birmingham, Alabama 35203
Tel. (205) 855-5700
ehare@dicellolevitt.com

FREESE & GOSS PLLC
Richard A. Freese

Jackson A. Freese
Regions Harbert Plaza
1901 6th Avenue North, Ste. 3120
Birmingham, Alabama 35203
rich@freeseandgoss.com
jackson@freeseandgoss.com
Tel.: (205) 871-4144

Harlan F. Winn (WIN023)
Adam P. Plant (PLA005)
Battle & Winn LLP
2901 Second Avenue South, Suite 220
Birmingham, Alabama 35233
Tel: (205) 397-8160
Fax: (205) 397-8179
hwinn@battlewinn.com
aplant@battlewinn.com

Counsel for Plaintiffs and the Proposed Class