AlaFile E-Notice

01-CV-2025-902264.00

To: JONATHAN S. MANN
jonm@pittmandutton.com

NOTICE OF ELECTRONIC FILING

IN THE CIRCUIT COURT OF JEFFERSON COUNTY, ALABAMA

JOSEPH LODICO V. BRADFORD HEALTH SERVICES, LLC
01-CV-2025-902264.00

The following complaint was FILED on 9/29/2025 9:08:28 PM

Notice Date: 9/29/2025 9:08:28 PM

JACQUELINE ANDERSON SMITH
CIRCUIT COURT CLERK
JEFFERSON COUNTY, ALABAMA
716 RICHARD ARRINGTON, JR BLVD
BIRMINGHAM, AL, 35203

205-325-5355
jackie.smith@alacourt.gov

ELECTRONICALLY FILED
9/29/2025 9:08 PM
01-CV-2025-902264.00
CIRCUIT COURT OF
JEFFERSON COUNTY, ALABAMA
JACQUELINE ANDERSON SMITH, CLERK

IN THE CIRCUIT COURT OF JEFFERSON COUNTY, ALABAMA
BIRMINGHAM DIVISION

IN RE BRADFORD HEALTH SERVICES, LLC DATA BREACH LITIGATION	Master File No. 01-CV-2025-902264.00.
This Document Relates To: ALL ACTIONS	**CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiffs Richard Hussey, Joseph Lodico, James Brooks, and Lorna Bell (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this Consolidated Class Action Complaint against Bradford Health Services, LLC ("BHS") and Bradford Health Partners, LLC ("BHP", and collectively, "Defendants"), alleging as follows based upon personal knowledge, information and belief, and investigation of counsel.

NATURE OF ACTION

1. Plaintiffs brings this class action against Defendants for their failure to properly secure and safeguard protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), medical information, and other personally identifiable information ("PII") (collectively, "PII/PHI" or "Private Information"), and for failing to provide timely, accurate, and adequate notice to Plaintiffs and other Class Members (defined below) that the integrity of their PII/PHI had been compromised. Defendants' actions and inactions also violated the Alabama Data Breach Notification Act of 2018, specifically Ala. Code § 8-38-3 and Ala. Code § 8-38-5.

2. Defendant BHS is a provider of addiction treatment programs throughout

Alabama and the Southeast.

3. Defendant BHP is a provider of health care services and is based in Alabama.

4. As healthcare service providers, Defendants knowingly obtain sensitive patient and employee Private Information and have a resulting duty to securely maintain such information in confidence.

5. On December 8, 2023, Defendant BHS detected unusual activity within its IT Network.[1] In response, Defendant BHS launched an investigation to determine the nature and scope of the Data Breach.[2]

6. Defendant BHS' investigation determined that certain files stored on its network may have been accessed and acquired without authorization.[3] After a thorough review of those files, which concluded on May 15, 2025, Defendant BHS determined that certain individuals' Private Information may have been affected.[4]

7. Upon information and belief, the following types of Private Information were compromised as a result of the Data Breach: 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.[5]

8. On May 30, 2025, Defendants issued a notice of public disclosure about the Data Breach and began sending notice letters ("Notice") to impacted individuals.

[1] https://bradfordhealth.com/notice-of-data-security-incident/ (last visited Sept. 29, 2025).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*

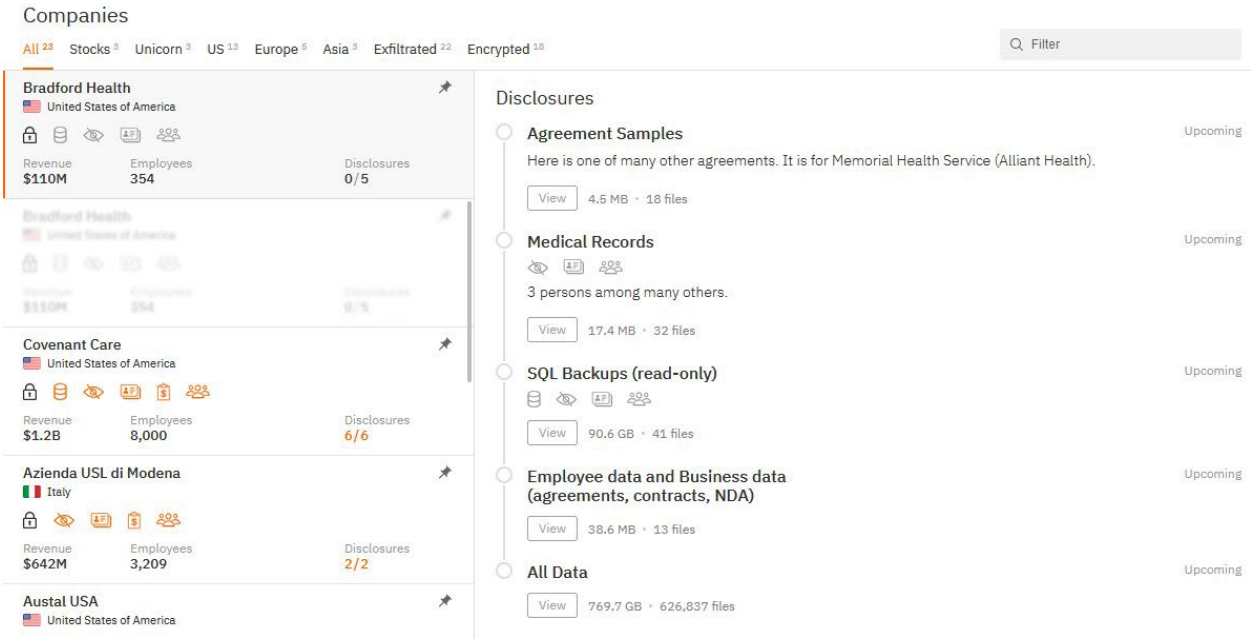
9. This Data Breach occurred because Defendants stored the electronic files containing the PII/PHI of Plaintiffs and hundreds of thousands of other Class Members unguarded, unprotected, unencrypted, and/or otherwise vulnerable to unauthorized access and theft by unauthorized third parties.

10. Despite the breadth and sensitivity of the PII/PHI that was exposed, and the attendant consequences to Class Members, as a result of the exposure, Defendants failed to disclose the Data Breach until May 30, 2025, ***eighteen months*** from the time it was first discovered, further exacerbating harm to its current and former patients and the Class.

11. This Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Class Members' PII and PHI.

12. After the Data Breach, ransomware group Hunters International claimed responsibility for the Data Breach and stated that they stole over 760 GBs from Defendants.[6]

[6] https://x.com/Comparitech/status/1929519619531792390/photo/1; *see also* https://www.comparitech.com/ransomware-attack-map/



13. Defendants disregarded the rights of Plaintiffs and Class Members by: intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard patients' and employees' PII and PHI; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach; and failing to provide effective credit protection services after notification of the Data Breach.

14. As a result of Defendants' failure to implement and follow basic security procedures, Plaintiffs and Class Members PII and PHI are now in the hands of thieves who, upon information and belief, have committed criminal acts against Class Members by misusing their data and/or have published their data on the internet for others to misuse. Plaintiffs and Class Members have had to spend, and will continue to spend significant amounts of time and money to protect themselves from the adverse ramifications of the Data Breach and will forever be at a

heightened risk of identity theft and financial fraud.

15. Plaintiffs, on behalf of all others similarly situated, allege claims for negligence/wantonness, negligence *per se*, breach of express and/or implied contracts, and unjust enrichment, and seeks to compel Defendants to fully and accurately disclose the nature of the Data Breach and the information that has been compromised, in addition to adopting reasonably sufficient security practices to safeguard patients and employees PII and PHI that remains in their custody in order to prevent incidents like the Data Breach from reoccurring in the future.

16. Defendants flagrantly disregarded Plaintiffs and the other Class Members' privacy rights by intentionally, willfully, recklessly, negligently and/or wantonly failing to take the necessary precautions required to safeguard and protect their PII/PHI from unauthorized disclosure.

17. Plaintiffs and Class Members' PII/PHI were improperly handled and stored and were otherwise not kept in accordance with federally prescribed, industry standard security procedures. As a result, Plaintiffs and Class Members' PII/PHI was compromised and/or stolen.

18. Defendants intentional, willful, reckless, negligent and/or wanton disregard of Plaintiffs and Class Members' rights directly and/or proximately caused a substantial unauthorized disclosure of Plaintiffs and Class Members' PII/PHI. The improper use of PII/PHI by unauthorized third parties resulted in an adverse impact on the credit rating and finances of Plaintiffs and the Class Members.

19. The type of wrongful PII/PHI disclosure made by Defendants is the most harmful because it generally takes a significant amount of time for a victim to become aware of misuse of that PII/PHI. Additionally, it takes a significant amount of time to protect oneself against actual identity theft and financial fraud.

20. On behalf of themselves and Class Members, Plaintiffs have suffered actual damages as a direct and/or proximate result of Defendants wrongful actions and/or inaction and the resulting Data Breach including, but not limited to, misuse of their PII/PHI, publication and dissemination of their PII/PHI on the internet, identity theft, financial fraud, loss of money and time in combatting the identity theft and fraud, and emotional distress.

21. Defendants' wrongful actions and/or inactions and the resulting Data Breach have placed Plaintiffs and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[7] Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released a 2012 Identity Fraud Report (the "Javelin Report") quantifying the impact of data breaches. According to the Javelin Report, individuals whose PII/PHI is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity theft and/or identity fraud has not yet been discovered or reported and a high probability that criminals who may now possess Plaintiffs and Class Members' PII/PHI—if they have not already misused the date—will do so later or re-sell it. Even if they were without such loss, Plaintiffs and Class Members are entitled to relief and recovery.

22. Defendants' wrongful actions and/or inactions constitute common law negligence and common law invasion of privacy by public disclosure of private facts. Further, Defendants' wrongful actions and/or inactions constitute a breach of contract and Defendants have been unjustly enriched.

[7] According to the United States Government Accounting Office, the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities, such as when PII/PHI is used to commit fraud or other crimes (credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services)).

23. Plaintiffs, on behalf of themselves and the Class Members, seek actual damages, economic damages, nominal damages, exemplary damages, injunctive relief, and costs of suit.

PARTIES

Plaintiff Richard Hussey

24. Plaintiff Richard Hussey is an adult resident citizen of Morgan County, Alabama, a former BHS patient, and suffered damages as set forth below.

25. Plaintiff Hussey received medical treatment and entrusted Defendants with his PII and PHI, and his PII/PHI was included in the Data Breach.

26. Upon information and belief, Plaintiff Hussey's PII/PHI, which he entrusted to Defendants and which Defendants failed to properly safeguard, was stolen from Defendants by unauthorized third parties.

27. As a direct and/or proximate result of Defendants wrongful actions and/or inactions and the resulting Data Breach, Plaintiff Hussey has suffered economic damages relating to the theft of his PII/PHI, and other actual harm, including but not limited to publication and dissemination of his PII/PHI on the internet, and emotional distress over learning of the theft of his PII/PHI. Defendants' wrongful disclosure of and failure to safeguard Plaintiff Hussey's PII/PHI has also placed him at an imminent, immediate, and continuing increased risk of harm for identity theft, financial fraud, and medical fraud.

Plaintiff Joseph Lodico

28. Plaintiff Joseph Lodico is an adult resident citizen of Jefferson County, Alabama, a former BHS Patient, and suffered damages as set forth below.

29. Plaintiff Lodico received medical treatment and entrusted Defendants with his PII and PHI, and his PII/PHI was included in the Data Breach.

30. Upon information and belief, Plaintiff Lodico's PII/PHI, which he entrusted to Defendants and which Defendants failed to properly safeguard, was stolen from Defendants by unauthorized third parties.

31. As a direct and/or proximate result of Defendants' wrongful actions and/or inactions and the resulting Data Breach, Plaintiff Lodico has suffered economic damages relating to the theft of his PII/PHI, and other actual harm, including but not limited to publication and dissemination of his PII/PHI on the internet, and emotional distress over learning of the theft of his PII/PHI. Defendants' wrongful disclosure of and failure to safeguard Plaintiff Lodico's PII/PHI has also placed him at an imminent, immediate, and continuing increased risk of harm for identity theft, financial fraud, and medical fraud.

Plaintiff James Brooks

32. Plaintiff James Brooks is an adult resident citizen of Mobile County, Alabama, a former BHS patient, and suffered damages as set forth below.

33. Plaintiff Brooks received medical treatment and entrusted Defendants with his PII and PHI, and his PII/PHI was included in the Data Breach.

34. Upon information and belief, Plaintiff Brook's PII/PHI, which he entrusted to Defendants and which Defendants failed to properly safeguard, was stolen from BHS by unauthorized third parties.

35. As a direct and/or proximate result of Defendants wrongful actions and/or inactions and the resulting Data Breach, Plaintiff Brooks has suffered economic damages relating to the theft of his PII/PHI, and other actual harm, including but not limited to publication and dissemination of his PII/PHI on the internet, and emotional distress over learning of the theft of his PII/PHI. Defendants' wrongful disclosure of and failure to safeguard Plaintiff's PII/PHI has

also placed him at an imminent, immediate, and continuing increased risk of harm for identity theft, financial fraud, and medical fraud.

Plaintiff Lorna Bell

36. Plaintiff Lorna Bell is an adult resident citizen of Madison County, Alabama, a former BHS employee, and suffered damages as set forth below.

37. Plaintiff Bell received employment services and entrusted Defendants with her PII and PHI, and his PII/PHI was included in the Data Breach.

38. Upon information and belief, Plaintiff Bell's PII/PHI, which she entrusted to Defendants and which Defendants failed to properly safeguard, was stolen from Defendants by unauthorized third parties.

39. As a direct and/or proximate result of Defendants wrongful actions and/or inactions and the resulting Data Breach, Plaintiff Bell has suffered economic damages relating to the theft of her PII/PHI, and other actual harm, including but not limited to publication and dissemination of her PII/PHI on the internet, and emotional distress over learning of the theft of her PII/PHI. Defendants' wrongful disclosure of and failure to safeguard Plaintiff Bell's PII/PHI has also placed her at an imminent, immediate, and continuing increased risk of harm for identity theft, financial fraud, and medical fraud.

Defendant BHS

40. Defendant BHS is a foreign limited liability company that has its principal place of business in Jefferson County, Alabama located at is 2101 Magnolia Avenue South, Suite 518, Birmingham, Alabama, 35205. Defendant BHS is registered and qualified to do business in Alabama, and was doing business in Jefferson County, Alabama at all times materially relevant hereto.

Defendant BHP

41. Defendant BHP is a foreign limited liability company that has its principal place of business in Jefferson County, Alabama located at 2101 Magnolia Ave South, Suite 518, Birmingham, Alabama, 35205. Defendant BHP is registered and qualified to do business in Alabama, and was doing business in Jefferson County, Alabama at all times materially relevant hereto.

JURISDICTION AND VENUE

42. Jurisdiction is proper in Alabama because, at all relevant times, Defendants conducted (and continue to conduct) business in Jefferson County, Alabama, Plaintiffs received services and contracted with Defendants to safeguard their PII and PHI in Alabama, many of Defendants wrongful acts and omissions took place in Alabama, and Defendants principal places of business at 2101 Magnolia Avenue South, Suite 518, Birmingham, AL 35205.

43. Venue is proper in Jefferson County, Alabama pursuant to Ala. Code §§ 6-3-7(a) and (b) because, at all relevant times, a substantial part of the events or omissions giving rise to this action occurred in Jefferson County, Defendants' principal place of business is 2101 Magnolia Avenue South, Suite 518, Birmingham, AL 35205, and Defendants conduct business throughout Jefferson County.

BACKGROUND

A. *Defendants Acquires, Collects, and Stores Plaintiffs and Class Members' PII/PHI*

26. In the regular course of its business, Defendants acquire, collect, store and maintain possession, custody, and control of a wide variety and massive amount of information of Plaintiffs and Class Members' personal and confidential information, including: names, dates of birth, Social Security numbers, health insurance information, treatment information, medical

record numbers, and medical history details.

27. As a condition of obtaining services from Defendants, Defendants require that patients and employees entrust them with highly sensitive personal information.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' PII/PHI, Defendants assumed legal and equitable duties to those individuals and knew or should have known that they were responsible for protecting Plaintiffs and Class Members' PII/PHI from disclosure.

29. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII/PHI. Plaintiffs and Class Members, as current and former patients and employees, relied on Defendants to keep their PII/PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

30. Upon information and belief, Defendants made promises and representations to patients and employees that the Private Information collected would be kept safe and confidential, the privacy of that information would be maintained.

31. Defendants had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendants have a legal duty to keep patients' and employees' Private Information safe and confidential.

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

33. Plaintiffs and Class Members provided their Private Information to Defendants

with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

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

35. By obtaining, collecting, using, and deriving a benefit from Plaintiffs and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs and Class Members' Private Information from disclosure.

B. *The Data Breach*

36. On December 8, 2023, Defendant BHS detected unusual activity within its IT Network.[8] In response, Defendant BHS launched an investigation to determine the nature and scope of the Data Breach.[9]

44. Defendant BHS' investigation determined that certain files stored on its network may have been accessed and acquired without authorization.[10] After a thorough review of those files, which concluded on May 15, 2025, Defendant BHS determined that certain individuals' Private Information may have been affected.[11]

45. Upon information and belief, the following types of Private Information were

[8] https://bradfordhealth.com/notice-of-data-security-incident/ (last visited Sept. 29, 2025).
[9] *Id.*
[10] *Id.*
[11] *Id.*

compromised as a result of the Data Breach: 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.[12]

46. On May 30, 2025, Defendants issued a notice of public disclosure about the Data Breach and began sending Notices to impacted individuals.

37. Defendants' Notices to Plaintiffs and Class Members fail to state when the unauthorized access began.

38. Given the unknown period of time during which unauthorized third parties had access to files—and the eighteen months between the discovery of the Data Breach and Defendants public disclosure of it—Plaintiffs and Class Members' PII/PHI has likely been bought and sold several times on the robust international cyber black market while Defendants denied Plaintiffs and Class Members any opportunity to take measures to protect their PII/PHI and privacy.

39. Defendants' wrongful actions and/or inactions—to wit, failing to protect Plaintiffs and Class Members' PII/PHI—directly and/or proximately caused the theft and dissemination into the public domain of Plaintiffs and Class Members' PII/PHI without their knowledge, authorization, and/or consent. As a further direct and/or proximate result of Defendants wrongful actions and/or inactions, Plaintiffs and Class Members have suffered, and will continue to suffer, damages including, without limitation: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure, dissemination and publication of their PII/PHI; (iii) criminal misuse of their PII/PHI; (iv) identity theft; (v) financial fraud; (vi) loss of privacy; (vii) out-of-

[12] *Id.*

pocket expenses incurred to mitigate the identity theft and financial fraud and the continued increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (viii) economic losses relating to the theft of their PII/PHI; (ix) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (x) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (xi) stress, anxiety and emotional distress.

40. As a result of Defendants' failure to properly safeguard and protect Plaintiffs and Class Members' PII/PHI, Plaintiffs and Class Members' privacy has been invaded and their rights violated. Their compromised PII/PHI was private and sensitive in nature and was left inadequately protected by Defendants. Defendants' wrongful actions and/or inactions and the resulting Data Breach have caused Plaintiffs and Class Members to suffer from identity theft and fraud, as well as placing them at a continuing increased risk of identity theft and identity fraud.

C. ***The Value of Personally Identifiable Information***

41. Identity theft occurs when a person's PII, such as the person's name, e-mail address, date of birth, Social Security number, billing and shipping addresses, phone number and credit card information is used without his or her permission to commit fraud or other crimes.[13]

42. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[14] Furthermore, "there is significant evidence demonstrating that technological

[13] *See What to Know About Identity Theft*, FED. TRADE COMM'N, https://consumer.ftc.gov/articles/what-know-about-identity-theft#what_is (last visited Sept. 29, 2025).
[14] *Protecting Consumer Privacy in an Era of Rapid Change FTC Report*, FED. TRADE COMM'N (March 2012) https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf) (last visited Sept. 29, 2025).

advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute [PII]."[15]

43. The FTC estimates that the identities of as many as 9 million Americans are stolen each year.[16]

44. As a direct and/or proximate result of the Data Breach, Plaintiffs and Class Members will now be required to spend money and to take the time and effort to combat actual identity theft and fraud and also mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, placing "freezes" and "alerts" with the credit reporting agencies, closing or modifying financial accounts, scrutinizing their bank and credit accounts and purchasing products to monitor their credit reports and accounts for unauthorized activity. Because Plaintiffs and Class Members' PII/PHI were stolen and/or compromised, they also now face a significantly heightened risk of identity theft.

45. According to the FTC, identity theft is serious. "[Identity thieves] might steal your name and address, credit card, or bank account numbers, Social Security number, or medical insurance account numbers. And they could use them to buy things with your credit cards, get new credit cards in your name, open a phone, electricity, or gas account in your name, steal your tax refund, use your health insurance to get medical care, [or] pretend to be you if they are arrested."[17]

46. Theft of medical information, such as that included in the Data Breach here, is equally serious: "Medical identity theft is when someone uses your personal information—like your name, Social Security number, health insurance account number or Medicare number—to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance

[15] *Id*. at 11–12.
[16] *Id.*
[17] *See What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER ADVICE https://consumer.ftc.gov/articles/what-know-about-identity-theft#what_is (last visited Sept. 29, 2025).

provider, or get other medical care. If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[18]

47. Identity thieves also use Social Security numbers to commit other types of fraud. The GAO found that identity thieves use PII/PHI to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, while in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PII/PHI, Social Security numbers are incredibly difficult to change, and their misuse can continue for years into the future.

48. Identity thieves also use Social Security numbers to commit other types of fraud, such as obtaining false identification cards, obtaining government benefits in the victim's name, committing crimes and/or filing fraudulent tax returns on the victim's behalf to obtain fraudulent tax refunds. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments, and/or obtain medical services in the victim's name. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

49. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that

[18] *See What to Know About Medical Identity Theft*, FED. TRADE COMM'N CONSUMER ADVICE https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Sept. 29, 2025).

someone is using the number fraudulently, as well as show that he has done all he can to fix the problems resulting from the misuse.[19] Thus, a person whose PII/PHI has been stolen cannot obtain a new Social Security number until the damage has already been done.

50. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems. Because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of credit history.

51. As a direct and/or proximate result of Defendants wrongful actions and/or inactions and the Data Breach, the thieves and/or their customers now have Plaintiffs and Class Members' PII/PHI. As such, Plaintiffs and Class Members have been deprived of the value of their PII/PHI.[20]

52. Plaintiffs and Class Members' PII/PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for a number of years.[21] Identity thieves and other cyber criminals openly post stolen Social Security numbers, and other personal financial information on various Internet websites, thereby making the information publicly available.

---

[19] *See* https://consumer.ftc.gov/articles/do-you-need-new-social-security-number (last visited Sept. 29, 2025).
[20] *See, e.g.,* John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted); *Your Medical Records May Not Be Private: ABC News Investigation*, ABC NEWS http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986&page=2#.UGRgtq7yBR4 (last visited Sept. 29, 2025).
[21] Companies, in fact, also recognize PII/PHI as an extremely valuable commodity akin to a form of personal property. *See* T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

53. The Data Breach was a direct and/or proximate result of Defendants failure to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect Plaintiffs and Class Members' PII/PHI from unauthorized access, use, and/or disclosure, as required by various state regulations and industry practices.

54. Defendants flagrantly disregarded and/or violated Plaintiffs and Class Members' privacy rights, and harmed them in the process, by not obtaining Plaintiffs and Class Members' prior written consent to disclose their PII/PHI to any other person—as required by HIPAA and other pertinent laws, regulations, industry standards and/or internal company standards.

55. Defendants flagrantly disregarded and/or violated Plaintiffs and Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical, and other safeguards required by both industry standards and the Alabama Data Breach Notification Act of 2018, Ala. Code 1975 § 8-38-3, to ensure the security and confidentiality of Plaintiffs and Class Members' PII/PHI to protect against anticipated threats to the security or integrity of such information. Defendants' security deficiencies allowed unauthorized individuals to access, remove from their servers and networks, disclose, and/or compromise the PII/PHI of hundreds of thousands of individuals—including Plaintiffs and Class Members.

56. Defendants' wrongful actions and/or inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs and Class Members' PII/PHI without their knowledge, authorization, and consent. As a direct and proximate result of Defendants wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and Class Members have incurred damages in the form of, *inter alia*: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure, dissemination and publication of their PII/PHI; (iii) criminal

misuse of their PII/PHI; (iv) identity theft; (v) financial fraud; (vi) loss of privacy; (vii) out-of-pocket expenses incurred to mitigate the identity theft and financial fraud and the continued increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (viii) economic losses relating to the theft of their PII/PHI; (ix) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (x) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (xi) stress, anxiety and emotional distress. Plaintiffs and Class Members' damages were foreseeable by Defendants.

D. *Defendants Conduct Violates HIPAA and Industry Standard Practices*

57. Title II of HIPAA contains what are known as 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 PII/PHI like the data Defendants left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

58. Defendants Data Breach resulted from a combination of insufficiencies that indicate Defendants failed to comply with safeguards mandated by HIPAA regulations and industry standards. Defendants' security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to adequately catalog the location of patients' and employees', including Plaintiffs and Class Members', digital information;

d. Failing to properly encrypt Plaintiffs and Class Members' PII/PHI;

e. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants create, receive, maintain, and transmit in violation of 45 CFR 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only

to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

h. 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 CFR 164.308(a)(6)(ii);

i. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

j. Failing to protect against any 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 CFR 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 CFR 164.306(a)(94);

l. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*;

m. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45 CFR 164.308(a)(5); and

n. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

PLAINTIFFS FACTS

Plaintiff Richard Hussey

59. Plaintiff Richard Hussey is a former patient of Defendant BHS. When Plaintiff first became a patient of Defendant BHS, he was required to provide Defendants with substantial amounts of his PII and PHI.

60. On or about May 30, 2025, Plaintiff received the Notice in the mail, which told him that his Private Information had been impacted during the Data Breach. Specifically, the Notice

stated that Plaintiff's "name, as well as your Social Security Number, health care dates of service, Medical Record Number (MRN)."

61. Plaintiff will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of his Private Information.

62. Plaintiff suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

63. Plaintiff would not have provided his Private Information to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard the personal information in their possession from theft, and that those systems were subject to a data breach.

64. Plaintiff suffered actual injury in the form of having his Private Information compromised, stolen, published on the dark web and/or sold by and to other cybercriminals as a result of the Data Breach.

65. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his personal information – a form of intangible property that Plaintiff was required to provide to Defendant for the purpose of being a patient and which was compromised, stolen and exfiltrated in, and as a result of, the Data Breach.

66. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his PII/PHI being placed in the hands of criminals.

67. Plaintiff has a continuing interest in ensuring that his PII/PHI, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

68. As a result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing financial accounts for any indications of actual or attempted identity theft or fraud, as well as long-term credit monitoring options he will now need to use. Plaintiff has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

69. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of his PII/PHI to cybercriminals, which Private Information he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his PII/PHI for purposes of committing cyber and other crimes against him. Plaintiff is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on his life.

70. Plaintiff also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendants obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

71. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff Joseph Lodico

72. Plaintiff Joseph Lodico is a former patient of Defendant BHS. When Plaintiff first became a patient of Defendant BHS, he was required to provide Defendants with substantial amounts of his PII and PHI.

73. On or about May 30, 2025, Plaintiff received the Notice in the mail, which told him that his Private Information had been impacted during the Data Breach. Specifically, the Notice stated that Mr. Lodico's "name, as well as your date of birth, physician name, health care dates of service, treatment information / diagnosis, Medical Record Number (MRN), and health insurance policy number.

74. Plaintiff will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of his Private Information.

75. Plaintiff suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

76. Plaintiff would not have provided his Private Information to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard the personal information in their possession from theft, and that those systems were subject to a data breach.

77. Plaintiff suffered actual injury in the form of having his Private Information compromised, stolen, published on the dark web and/or sold by and to other cybercriminals as a result of the Data Breach.

78. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his personal information – a form of intangible property that Plaintiff Lodico was required to provide to Defendants for the purpose of being a patient and which was compromised, stolen and exfiltrated in, and as a result of, the Data Breach.

79. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his PII/PHI being placed in the

hands of criminals.

80. Plaintiff has a continuing interest in ensuring that his PII/PHI, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

81. As a result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing financial accounts for any indications of actual or attempted identity theft or fraud, as well as long-term credit monitoring options he will now need to use. Plaintiff has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

82. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of his PII/PHI to cybercriminals, which Private Information he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his PII/PHI for purposes of committing cyber and other crimes against him. Plaintiff is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on his life.

83. Plaintiff also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendants obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

84. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff James Brooks

85. Plaintiff James Brooks is a former patient of Defendant BHS. When Plaintiff first became a patient of BHS, he was required to provide Defendants with substantial amounts of his PII and PHI.

86. On or about May 30, 2025, Plaintiff received the Notice in the mail, which told him that his Private Information had been impacted during the Data Breach.

87. Plaintiff will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of his Private Information.

88. Plaintiff suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

89. Plaintiff would not have provided his Private Information to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard the personal information in their possession from theft, and that those systems were subject to a data breach.

90. Plaintiff suffered actual injury in the form of having his Private Information compromised, stolen, published on the dark web and/or sold by and to other cybercriminals as a result of the Data Breach.

91. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his personal information – a form of intangible property that Plaintiff was required to provide to Defendants for the purpose of being a patient and which was compromised, stolen and exfiltrated in, and as a result of, the Data Breach.

92. Plaintiff suffered imminent and impending injury arising from the substantially

increased risk of future fraud, identity theft, and misuse posed by his PII/PHI being placed in the hands of criminals.

93. Plaintiff has a continuing interest in ensuring that his PII/PHI, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

94. As a result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing financial accounts for any indications of actual or attempted identity theft or fraud, as well as long-term credit monitoring options he will now need to use. Plaintiff has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

95. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of his PII/PHI to cybercriminals, which Private Information he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his PII/PHI for purposes of committing cyber and other crimes against him. Plaintiff is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on his life.

96. Plaintiff also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendants obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

97. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff Lorna Bell

98. Plaintiff Lorna Bell is a former employee of Defendant BHS. When Plaintiff first became an employee of Defendant BHS, she was required to provide Defendants with substantial amounts of her PII and PHI.

99. On or about May 30, 2025, Plaintiff received the Notice in the mail, which told her that her Private Information had been impacted during the Data Breach.

100. Plaintiff will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

101. Plaintiff suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

102. Plaintiff would not have provided her Private Information to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard the personal information in their possession from theft, and that those systems were subject to a data breach.

103. Plaintiff suffered actual injury in the form of having her Private Information compromised, stolen, published on the dark web and/or sold by and to other cybercriminals as a result of the Data Breach.

104. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her personal information – a form of intangible property that Plaintiff was required to provide to Defendants for the purpose of being an employee and which was compromised, stolen and exfiltrated in, and as a result of, the Data Breach.

105. Plaintiff suffered imminent and impending injury arising from the substantially

increased risk of future fraud, identity theft, and misuse posed by her PII/PHI being placed in the hands of criminals.

106. Plaintiff has a continuing interest in ensuring that her PII/PHI, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

107. As a result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing financial accounts for any indications of actual or attempted identity theft or fraud. Plaintiff has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

108. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of his PII/PHI to cybercriminals, which Private Information he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his PII/PHI for purposes of committing cyber and other crimes against her. Plaintiff is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on his life.

109. Plaintiff also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendants obtained from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

110. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

111. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

112. Plaintiffs and Class Members entrusted their Private Information to Defendants in order to provide services and/ or receive Defendants services.

113. Plaintiffs Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendants inadequate data security practices.

114. As a direct and proximate result of Defendants actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

115. Further, as a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

116. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

117. The PII/PHI maintained by and stolen from Defendants systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

118. Plaintiffs and Class Members also lost the benefit of the bargain they made with

Defendants. Plaintiffs and Class Members overpaid for services or received less wages than what they ought to have received, when Defendants provided them with inadequate data security. Indeed, part of the price patients paid to Defendants, and wages withheld from employees, were intended to be used by Defendants to fund adequate security systems and protect Plaintiffs and Class Members Private Information.

119. Additionally, as a direct and proximate result of Defendants conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

120. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

121. Additionally, Plaintiffs and Class Members also suffered a loss of value of their PII/PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[22] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[23]

---

[22] *See How Data Brokers Profit from the Data We Create*, THE QUANTUM RECORD (Apr. 5, 2023), https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on Sept. 29, 2025).

[23] *Frequently Asked Questions,* NIELSEN COMPUTER & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Sept. 29, 2025).

122. As a result of the Data Breach, Plaintiffs and Class Members' PII/PHI, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

123. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. The contractual bargain entered into between Plaintiffs and Defendants included Defendants contractual obligation to provide adequate data security, which Defendants failed to provide. Thus, Plaintiffs and Class Members did not get what they bargained for.

124. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

d. Contacting financial institutions and closing or modifying financial accounts;

e. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones; and

f. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

125. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII/PHI, which is believed to still be in the possession of Defendants, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

126. As a direct and proximate result of Defendants actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

CLASS ACTION ALLEGATIONS

127. Pursuant to Rule 23 of the Alabama Rules of Civil Procedure, Plaintiffs bring this consolidated class action complaint as a nationwide class action on behalf of themselves and the following Class of similarly situated individuals:

> All persons residing in the United States whose personal identifying information (PII) and/or personal health information (PHI) was exposed to unauthorized third parties as a result of the Data Breach.

128. Excluded from the Class are the (i) owners, officers, directors, employees, agents and/or representatives of Defendants and their parent entities, subsidiaries, affiliates, successors, and/or or assigns, and (ii) the Court, Court personnel, and members of their immediate families.

129. The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Defendants, upon information

and belief, thousands of individuals were impacted. The Class is apparently identifiable within Defendants records, and Defendants have already identified these individuals (as evidenced by sending them breach notification letters).

130. The rights of each Class Member were violated in a virtually identical manner as a result of Defendants' willful, reckless, and/or negligent actions and/or inaction.

131. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a) Whether Defendants' willfully, recklessly, and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiffs and Class Members' PII/PHI;

b) Whether Defendants were negligent in the manner in which they stored Plaintiffs and Class Members' PII/PHI;

c) Whether Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in protecting and securing their PII/PHI;

d) Whether Defendants breached their duty to exercise reasonable care in protecting and securing Plaintiffs and Class Members' PII/PHI;

e) Whether Defendants were negligent in failing to secure Plaintiffs and Class Members' PII/PHI;

f) Whether Defendants' failure to comply with HIPAA constitutes negligence *per se*;

g) Whether Defendants failure to comply with Section 5 of the Federal Trade Commission Act (15 U.S.C. §45) negligence *per se*;

h) Whether Defendants failure to comply with the Alabama Data Breach Notification Act of 2018 constitutes negligence *per se*;

i) Whether Defendants breached their contracts by failing to maintain the privacy and security of Plaintiffs and Class Members' PII/PHI;

j) Whether by publicly disclosing Plaintiffs and Class Members' PII/PHI without authorization, Defendants invaded Plaintiffs and Class Members' privacy; and,

k) Whether Plaintiffs and Class Members sustained damages as a result of Defendants' failure to secure and protect their PII/PHI.

132. Plaintiffs' claims are typical of Class Members' claims in that Plaintiffs claims and Class Members' claims all arise from Defendants failure to properly secure and protect Plaintiffs and Class Members' PII/PHI and the resulting Data Breach.

133. Plaintiffs and their counsel will fairly and adequately represent the interests of Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, Class Members' interests. Plaintiffs' lawyers are experienced litigators and intend to vigorously prosecute this action on behalf of Plaintiffs and Class Members.

134. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiffs and Class Members' claims. Plaintiffs and Class Members have been irreparably harmed as a result of Defendants wrongful actions and/or inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendants' failure to secure and protect Plaintiffs and Class Members' PII/PHI.

135. Class certification, therefore, is appropriate pursuant to ALA.R.CIV.P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

136. Class certification also is appropriate pursuant to ALA.R.CIV.P. 23(b)(2) because

Defendants have acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the class as a whole.

137. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights.

CAUSES OF ACTION

COUNT I
NEGLIGENCE/WANTONNESS
(On Behalf of Plaintiffs and the Class)

138. Plaintiffs re-allege and incorporate by reference paragraphs 1 – 137, as if fully set forth herein.

139. Defendants had a duty to exercise reasonable care in safeguarding and protecting Plaintiffs and Class Members' PII/PHI.

140. Defendants negligently and/or wantonly violated their duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs and Class Members' PII/PHI (as set forth in detail above).

141. Alternatively, Defendants' conduct set forth herein was so reckless and so charged with indifference to the consequences of its failure to exercise reasonable care in safeguarding and protecting Plaintiffs and the Class Members' PII/PHI (as set forth above) as to amount to wantonness under Alabama law.

142. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiffs and Class Members' PII/PHI would result in an unauthorized third-party gaining access to such information for no lawful purpose.

143. Plaintiffs and the Class Members were (and continue to be) damaged as a direct and/or proximate result of Defendants failure to secure and protect their PII/PHI in the form of,

inter alia, (i) improper disclosure of their PII/PHI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress—for which they are entitled to compensation.

144. Defendants' wrongful actions and/or inaction (as described above) constituted negligence and/or wantonness at common law.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

145. Plaintiffs re-allege and incorporate by reference paragraphs 1 – 137, as if fully set forth herein.

146. Federal and state statutory law and applicable regulations, including HIPAA's Privacy Rule, Section 5 of the Federal Trade Commission Act (15 U.S.C. §45), and the Alabama Data Breach Notification Act of 2018, set forth and otherwise establish duties in the industry that were applicable to Defendants and with which Defendants were obligated to comply at all relevant times hereto.

147. Defendants violated these duties by failing to safeguard and protect the Plaintiffs and Class Members' PII/PHI, which resulted in an unauthorized disclosure of the Plaintiffs and the Class Members' PII/PHI.

148. Subsection 8-38-3(a) of the Alabama Data Breach Notification Act of 2018 imposes a clear duty on healthcare entities like Defendants to protect PII/PHI: "Each covered entity and

third-party agent shall implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security."

149. Defendants breached this duty owed to Plaintiffs and the Class Members under Subsection 8-38-3(a) of the Alabama Data Breach Notification Act of 2018 by failing to implement and maintain reasonable security measures to protect their sensitive personally identifying information against a breach of security.

150. The purpose of HIPAA's Privacy Rule is to define and limit the circumstances in which the protected health information of individuals such as the Plaintiff and Class Members may be used or disclosed. The stated purpose of HIPAA's Privacy Rule was also to establish minimum standards for safeguarding the privacy of individually identifiable health information.

151. Defendants were also prohibited by the FTC Act from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015). Various FTC publications and orders also form the basis of Defendants' duty.

152. Defendants violated Section 5 of the FTC Act by failing to maintain reasonable and appropriate data security for their patients and employees PII and PHI.

153. The unauthorized disclosure of the Plaintiffs and Class Members' PII/PHI at issue in this action was exactly the type of conduct that the legislation referenced above was intended to prohibit, and the harm at issue in this case that has been suffered by the Plaintiffs and Class Members is the type of harm the legislation referenced above was intended to prevent.

154. Plaintiffs and Class Members, as owners of the sensitive personally identifying information that Defendants failed to protect, fall within the class of persons HIPAA's Privacy Rule, the FTC Act and the Alabama Data Breach Notification Act were intended to protect.

155. Subsection 8-38-5(b) of the Alabama Data Breach Notification Act of 2018 further imposes a clear duty on healthcare entities like Defendants to promptly notify affected persons so that the persons can take action to protect themselves: "[T]he covered entity shall provide notice within 45 days of . . . the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates."

156. Defendants breached their duty to promptly notify Plaintiffs and Class Members by failing to send out notification letters until approximately eighteen months after the Data Breach was purportedly discovered.

157. The harm suffered and that may be suffered in the future by the Plaintiffs and Class Members is the same type of harm HIPAA's Privacy Rule, the FTC Act and the Alabama Data Breach Notification Act of 2018 were intended to guard against.

158. As a direct and proximate result of Defendants violation of HIPAA's Privacy Rule and the Alabama Data Breach Notification Act of 2018, Plaintiffs and Class Members were damaged in the form of, without limitation, expenses for credit monitoring and insurance, expenses for periodic credit reports, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and noneconomic harm.

COUNT III
BREACH OF EXPRESS OR IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

159. Plaintiffs re-allege and incorporate by reference paragraphs 1 – 137, as if fully set forth herein.

160. Defendants had a written understanding with the Plaintiffs and the Class Members that they would not disclose Plaintiffs or Class Members' confidential information in a manner not authorized by applicable law or industry standards.

161. For example, Defendant BHS's Notice of Privacy Practices provided to Plaintiffs and the Class Members constitutes an express contract or at the very least created a meeting of the minds that was inferred from the conduct of the parties. Plaintiffs and the Class Members fully discharged their obligations under the contract.

162. Further, Alabama law imposes on physicians and medical providers an implied contract of confidentiality that is breached by the unauthorized release of medical information, and Defendants breached those implied contracts with Plaintiffs and Class Members when they released their PII/PHI to unauthorized third parties.

163. Defendants breached their contracts with the Plaintiffs and the Class Members by failing to safeguard and protect Plaintiffs and the Class Members' PII/PHI such that an unauthorized disclosure of Plaintiffs and the Class Members' PII/PHI occurred.

164. As a direct and proximate result of Defendants breach of their contracts with the Plaintiffs and the Class Members, Plaintiffs and the Class Members have been damaged in an amount to be proven at trial.

165. As further damages, Plaintiffs and the Class Members request restitution and costs of mitigation including, but necessarily limited to, the purchase of credit monitoring, credit insurance, periodic credit reports and expenses associated with the loss or replacement of their valuable PII/PHI included in the Data Breach.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

166. Plaintiffs re-allege and incorporate by reference paragraphs 1 – 137, as if fully set forth herein.

167. This Count is pleaded in the alternative to the breach of implied contract (Count III).

168. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they provided their monies or labor to Defendants and/or their agents and in so doing also provided Defendants with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendants the treatment that was the subject of the transactions and should have had their Private Information protected with adequate data security.

169. Defendants knew that Plaintiffs and Class Members conferred a benefit upon it and had accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendants profited from Plaintiffs retained data and used Plaintiffs and Class Members' Private Information for business purposes.

170. Defendants failed to secure Plaintiffs and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

171. Defendants acquired Private Information through inequitable record retention as they failed to investigate and/or disclose the inadequate data security practices previously alleged.

172. If Plaintiffs and Class Members had known that Defendants would not use adequate and reasonable data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information ti Defendants or obtained services from Defendants.

173. Plaintiffs and Class Members have no adequate remedy at law.

174. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants decision to prioritize their own profits over the requisite security and the safety of their Private Information.

175. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon them.

176. As a direct and proximate result of Defendants conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiffs Private Information being disseminated on the dark web, according to Experian; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

177. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their unlawful and wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

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

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the class, respectfully request that the Court enter judgment in Plaintiffs' favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, nominal damages and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard Private Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY DEMAND

Plaintiffs, on behalf of themselves and all others similarly situated, respectfully demand a trial by jury on all of the claims and causes of action so triable.

Dated: September 29, 2025

Respectfully submitted,

/s/ Jon Mann

Jonathan S. Mann (MAN057)
Austin B. Whitten (WHI165)
PITTMAN, DUTTON, HELLUMS, BRADLEY & MANN, P.C.
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Tel: (205) 322-8880
Fax: (205) 328-2711
Email: jonm@pittmandutton.com
Email: austinw@pittmandutton.com

Gary M. Klinger (*pro hac vice pending*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

Jeff Ostrow (*pro hac vice pending*)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
ostrow@kolawyers.com

Interim Co-Lead Class Counsel

CERTIFICATE OF SERVICE

I hereby certify that on September 29, 2025, I electronically filed the foregoing with the Clerk of Court using the AlaFile system, which will send notification of such filing to all counsel of record.

Joseph R. Duncan, Jr.
CLARK, MAY, PRICE, LAWLEY, DUNCAN & PAUL, LLC
3070 Green Valley Road
P.O. Box 43408
Birmingham, Alabama 35243
Tel: (205) 267-6601
Email: jduncan@clarkmayprice.com

Attorney for Defendants

/s/ Jon Mann
Of Counsel