ELECTRONICALLY FILED
6/26/2024 4:26 PM
01-CV-2024-902563.00
CIRCUIT COURT OF
JEFFERSON COUNTY, ALABAMA
JACQUELINE ANDERSON SMITH, CLERK

IN THE CIRCUIT COURT OF JEFFERSON COUNTY, ALABAMA
BIRMINGHAM DIVISION

JEREMY HUFSTETLER, ADAM RUNK, CONNIE HATFIELD, YASHVANTSINH JHALA, DALE STARK, LISA KENNY, A'TAVION MORRISSETTE, GENE SAWYER, ROBERT MOFFA, LEAH HARNER, and JUDY YOUNG, individually and on behalf of all others similarly situated,	)	**CASE NO.: _____**
Plaintiffs,	)	**JURY TRIAL DEMANDED**
v.	)	
UPSTREAM REHABILITATION, INC. and UPSTREAM ROLLCO, LLC,	)	
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiffs Jeremy Hufstetler, Adam Runk, Connie Hatfield, Yashvantsinh Jhala, Dale Stark, Lisa Kenny, A'Tavion Morrissette, Gene Sawyer, Robert Moffa, Leah Harner, and Judy Young, on behalf of themselves and all other individuals similarly situated, file this Class Action Complaint against Defendants Upstream Rehabilitation, Inc. and Upstream RollCo, LLC (collectively, "Upstream" or "Defendants") and allege as follows:

NATURE OF THE CASE

1. Plaintiffs bring this class action against Upstream Rehabilitation, Inc. and Upstream RollCo, LLC for its failure to properly secure and safeguard personally identifiable information ("PII"), protected health information ("PHI"), as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), other medical and financial information, (collectively, "PII/PHI"), and for failing to provide timely, accurate, and adequate notice to

Plaintiffs and other individuals who are Class Members (defined below) that the integrity of their PII/PHI had been compromised and stolen. Upstream's 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. Upon information and belief, at all times relevant hereto, Upstream claims their "specialized services lead the way in providing physical therapy management solutions, creating strong worker compensation networks and connecting health plans and benefit administrators with a growing network of physical, occupational and speech therapists across the United States."[1]

3. On or about September 15, 2023, Upstream notified its current and former patients (collectively, "Patients") that unauthorized third parties accessed its networks and servers that contained Patients' private and sensitive PII/PHI including, but not limited to, full names, dates of birth, contact information, demographic information, medical information, health insurance information, and/or Social Security number ("Data Breach"). A copy of the data breach notification letter that Upstream sent to its Patients is attached hereto as **Exhibit A**.

4. On January 24, 2023, Upstream discovered that unauthorized third parties accessed, viewed, and stole the PII/PHI of several Patients from its computer networks, systems and/or servers. This occurred because Upstream stored the electronic files containing the PII/PHI of Plaintiffs and other Alabama citizens who are Class Members without proper cybersecurity measures in place—the files were unguarded, unprotected, unencrypted, and/or otherwise vulnerable to unauthorized access and theft by unauthorized third parties.

5. Despite the breadth and sensitivity of the PII/PHI that was exposed, and the attendant consequences to Patients as a result of the exposure, Upstream failed to disclose the

[1] *Upstream Rehabilitation, Specialized Services: https://urpt.com/specialized-services (Last accessed June 20, 2024).*

Data Breach for ***almost 8 months*** from the time it was first discovered, further exacerbating harm to its Patients.

6. This Data Breach was a direct result of Upstream's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Patients' PII/PHI.

7. Upstream disregarded the rights of Plaintiffs and Class Members by: intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data networks, systems and/or servers were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Patients' PII/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 comprehensive and effective credit protection services after notification of the Data Breach.

8. As a result of Upstream's failure to implement and follow basic security procedures, Upstream's Patients' PII/PHI is now in the hands of thieves who, upon information and belief, have committed criminal acts against the Patients by misusing their data and/or have published and/or sold their data on the internet (i.e., the "dark web") for others to view, access, and/or 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.

9. Plaintiffs, on behalf of all other citizens of Alabama similarly situated, allege claims for negligence, wantonness, negligence *per se*, breach of express and/or implied contracts, breach of fiduciary duty, breach of confidence, and unjust enrichment and seek to compel Upstream to fully and accurately disclose the nature of the Data Breach and the information that

has been compromised, in addition to adopting sufficient security practices and protocols to safeguard the Patients' PII/PHI that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future, because the risk of future harm from another Upstream data breach is both imminent and substantial.

10. Upstream disclosed to its Patients that unauthorized third parties had access to its networks and servers for weeks, which was more than sufficient time to access and steal Plaintiffs' and Class Members' PII/PHI, leading to an imminent and substantial risk of identity theft and other misuse of the Plaintiffs' information.

11. Upstream 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.

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

13. Upstream's 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.

14. The type of wrongful PII/PHI disclosure made by Upstream is the most harmful because it generally takes a significant amount of time for a data breach victim to become aware

of misuse of that PII/PHI. Additionally, it takes a significant amount of time to protect oneself against attempted and actual identity theft and financial fraud.

15. On behalf of themselves and Class Members, Plaintiffs bring this lawsuit because they have suffered, and will continue to suffer, actual injuries and damages as a direct and/or proximate result of Upstream's wrongful actions and/or inactions and the resulting Data Breach including, but not limited to, unauthorized disclosure, publication, and dissemination of their PII/PHI on the internet, misuse of their PII/PHI, identity theft, financial fraud, loss of money and time in combatting the attempted and actual identity theft and fraud, and emotional distress.

16. Additionally, Plaintiffs seek injunctive relief as a direct and/or proximate result of Upstream's wrongful actions and/or inactions to prevent Upstream's next data breach, which is both likely and imminent.

17. Upstream's wrongful actions and/or inactions and the resulting Data Breach have placed Plaintiffs and Class Members at an imminent, immediate, substantial, and continuing increased risk of identity theft and identity fraud.[2] 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 now possess Plaintiffs' and Class Members' PII/PHI—if they have not already

[2] 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)).

misused the data—will do so later or re-sell it. Even if they are without such loss now, Plaintiffs and Class Members are entitled to relief and recovery because Plaintiffs and Class Members are under an imminent risk that their information will soon be misused similar to the misuse other Plaintiffs have already experienced.

18. Upstream's wrongful actions and/or inactions constitute common law negligence and common law invasion of privacy by public disclosure of private facts. Further, Upstream's wrongful actions and/or inactions constitute a breach of contract, breach of fiduciary duty, breach of confidence, and unjust enrichment.

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

JURISDICTION AND VENUE

20. Jurisdiction is proper in Alabama because, at all relevant times, Upstream conducted (and continues to conduct) business in Alabama, each Plaintiff received health services and contracted with Upstream to safeguard their PII and PHI in Alabama, Plaintiffs' PII/PHI was stored on Upstream's computer networks, systems and/or servers in Alabama, many of Upstream's wrongful acts and omissions took place in Alabama, Upstream's principal place of business is in Alabama, and, Upstream's limited liability company members are Alabama corporations, entities, or citizens.

21. Venue is proper in Jefferson County because a substantial part of the events or omissions giving rise to this action occurred in Jefferson County, Upstream's principal place of business is in Jefferson County, Upstream conducts business throughout Jefferson County, and Upstream's limited liability company members are Jefferson County, Alabama, corporations or resident citizens.

PARTIES

Plaintiff Jeremy Hufstetler

22. Plaintiff Hufstetler is an adult individual and, at all times relevant herein, a resident and citizen of the State of Georgia. Plaintiff Hufstetler is a victim of the Data Breach. Defendants received Plaintiff Hufstetler's PHI/PII in connection with the services he received at Upstream Rehabilitation.

23. Plaintiff Hufstetler is very careful about sharing his sensitive information. Plaintiff Hufstetler stores any documents containing his Private Information in a safe and secure location. he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. To his knowledge, neither his PII or PHI has ever been exposed in any other data breach.

24. Because of the Data Breach, Plaintiff Hufstetler's Private Information is now in the hands of cyber criminals.

25. Plaintiff Hufstetler suffered actual injury from the exposure and theft of his PII/PHI—which violates his rights to privacy.

26. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Hufstetler is now imminently at risk of crippling future identity theft and fraud.

27. As a result of the Data Breach, Plaintiff Hufstetler has had no choice but to spend numerous hours attempting to ameliorate, mitigate, and address the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Hufstetler has devoted time to investigating the Data Breach, regularly monitoring his credit, reviewing account statements and other information, and taking other steps in an attempt to

mitigate the harm caused by the Data Breach.

28. The letter Plaintiff Hufstetler received from Defendants specifically directed him to take the actions described above. Indeed, the Upstream breach letter stated: "We encourage you to remain vigilant against incidents of theft and fraud by reviewing account statements and explanation of benefits and monitoring free credit reports for suspicious activity and to detect errors."[3] The letter then listed several additional "steps" that victims of the Data Breach could take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing freezes on credit reports, contacting the FTC and state Attorneys General, and obtaining information about identity theft and frauds.[4]

29. Plaintiff Hufstetler is made uncomfortable because his personal information and all of his health information is in the hands of unauthorized individuals.

Plaintiff A'Tavion Morrissette

30. Plaintiff A'Tavion Morrissette is and has been, at all relevant times, a resident and citizen of Shelby, County, Alabama.

31. In exchange for medical services, Plaintiff Morrissette entrusted his Private Information to Defendants. Pursuant to HIPAA, Upstream was required to protect and maintain the confidentiality of Private Information entrusted to it.

32. Plaintiff Morrisette received a notice letter from Defendants dated September 15, 2023, informing him that his Private Information—including his PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

33. Plaintiff Morrissette is very careful about sharing his sensitive information.

[3] *See* https://consumer.sc.gov/sites/consumer/files/Documents/Security%20Breach%20Notices/UpstreamRollCoLLC.pdf (sample breach letter).
[4] *Id.*

Plaintiff Morrissette stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. To his knowledge, neither his PII or PHI has ever been exposed in any other data breach.

34. Plaintiff Morrissette and Class Members' Private Information was entrusted to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

35. Because of the Data Breach, Plaintiff Morrissette's Private Information is now in the hands of cyber criminals.

36. Plaintiff Morrissette suffered actual injury from the exposure and theft of his PII/PHI—which violates his rights to privacy.

37. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Morrissette is now imminently at risk of crippling future identity theft and fraud.

38. Since the Data Breach, Plaintiff Morrissette has experienced data misuse and identity theft. Specifically, Plaintiff Morrissette experienced unauthorized charges on his debit card in the spring and summer of 2023—just months after the Data Breach. Plaintiff Morrissette believes these unauthorized charges are plausibly attributable to the Data Breach, given the proximity of the charges to the Breach, that Plaintiff Morrissette is very careful with his Private Information, and that his Private Information has not been exposed in any other data breach.

39. As a result of the Data Breach, Plaintiff Morrissette has had no choice but to spend numerous hours attempting to ameliorate, mitigate, and address the harms caused by the Data

Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Morrissette has devoted time to investigating the Data Breach, researching how best to ensure that he is protected from identity theft, reviewing account statements and other information, and taking other steps in an attempt to mitigate the harm caused by the Data Breach.

40. The letter Plaintiff Morrissette received from Defendants specifically directed him to take the actions described above. Indeed, the Upstream breach letter stated: "We encourage you to remain vigilant against incidents of theft and fraud by reviewing account statements and explanation of benefits and monitoring free credit reports for suspicious activity and to detect errors."[5] The letter then listed several additional "steps" that victims of the Data Breach could take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing freezes on credit reports, contacting the FTC and state Attorneys General, and obtaining information about identity theft and frauds.[6]

41. As a result of the Data Breach, Plaintiff Morrissette has experienced a noticeable increase in anxiety due to the loss of his privacy and anxiety over the impact of cybercriminals accessing and misusing his Private Information.

42. Plaintiff Morrissette anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

Plaintiff Gene Sawyer

43. Plaintiff Gene Sawyer Sawyer is and has been, at all relevant times, a resident and citizen of Ringgold, Georgia.

44. Plaintiff Sawyer obtained medical services from Defendants in or about 2022.

45. In order to obtain medical services from Defendants, Plaintiff Sawyer was required

to provide his Private Information to Defendants.

46. Upon information and belief, at the time of the Data Breach—January 24, 2023 through January 31, 2023 and February 3, 2023 through February 9, 2023—Defendants retained Plaintiff Sawyer's Private Information in its system.

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

48. Plaintiff Sawyer received the Notice Letter, by U.S. mail, directly from Defendants, dated September 15, 2022. According to the Notice Letter, Plaintiff Sawyer's PII and PHI was improperly accessed and obtained by unauthorized third parties, including his name, diagnosis, health insurance subscriber number, medical record number, health insurance information, patient account number, and treatment information.

49. As a result of the Data Breach, and at the direction of Defendants' Notice Letter, Plaintiff Sawyer made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter as well as checking his financial accounts for any indication of unauthorized activity, which may take years to detect—valuable time that Plaintiff Sawyer otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

50. Plaintiff Sawyer suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of 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; and (vii) the continued and certainly increased risk to his 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.

51. The Data Breach has caused Plaintiff Sawyer to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

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

53. As a result of the Data Breach, Plaintiff Sawyer is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

54. Plaintiff Sawyer has a continuing interest in ensuring that his Private Information, which, upon information and belief, remain backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Robert Moffa

55. Plaintiff Robert Moffa is and has been, at all relevant times, a resident and citizen of Marietta, Georgia.

56. When Plaintiff Moffa became a patient, Defendants required that he provide substantial amounts of his PII and PHI.

57. On or about September 15, 2023, Plaintiff Moffa received a letter which told him that his PII and PHI had been impacted during the Data Breach. The notice letter informed him that the information stolen included his name, medical record number, health insurance information, patient account number, and treatment information.

58. The notice letter offered Plaintiff Moffa only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Moffa has already experienced (and will continue to experience) a substantial, continuous, and increased risk of identity theft, including but not limited to, potential identify theft and medical fraud.

59. Because of Defendants' failure to safeguard Plaintiff Moffa's PII and PHI, a criminal third-party has already attempted to enroll in auto insurance and apply for a car loan in his name without his authorization.

60. To the best of his knowledge, other than Defendants' Data Breach Plaintiff Moffa's PII and PHI have not been included in any other data breaches or otherwise been accessed without authorization.

61. In In addition, Plaintiff Moffa has suffered actual injury in the form of time spent monitoring his accounts for fraud and dealing with and attempting to mitigate the devastating impact the Data Breach has already had on his life, including but not limited to, the actual and increased risk of fraud he has experienced resulting from the Data Breach. Defendants specifically instructed Plaintiff Moffa to devote time and effort responding to the Data Breach.

62. Plaintiff Moffa would not have provided his PII and PHI to Defendants had Defendants timely disclosed that its systems lacked adequate computer and data security practices to safeguard its patients' personal and health information from theft, and that those systems were subject to multiple data breaches.

Plaintiff Leah Harner

63. Plaintiff Leah Harner is and has been, at all relevant times, a resident and citizen of Spokane, Washington.

64. Plaintiff Harner is unsure how Defendants came into possession of her PII/PHI, but believes it was through one of Defendants' physical therapy brands where she received treatment.

65. When Plaintiff Harner became a patient, she was required to provide Defendants with substantial amounts of her PII and PHI.

66. On or about September 15, 2023, Plaintiff Harner received a letter which told her that her PII and PHI had been impacted during the Data Breach. The notice letter informed her that the PII stolen included her name, medical billing information, medical record number, patient account number, and treatment information.

67. The notice letter offered Plaintiff Harner only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Harner will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

68. Plaintiff Harner suffered actual injury in the form of multiple unauthorized charges on her payment card totaling roughly $200, as well as the time spent contacting her bank regarding the fraudulent charges and otherwise dealing with the Data Breach and the increased risk of fraud resulting therefrom. The letter Plaintiff received from Defendants specifically directed her to take these actions.

69. Plaintiff Harner would not have provided her PII and PHI to Defendants had Defendants timely disclosed that its systems lacked adequate computer and data security practices

to safeguard its patients' personal and health information from theft, and that those systems were subject to multiple data breaches.

Plaintiff Connie Hatfield

70. Plaintiff Connie Hatfield is and has been, at all relevant times, a resident and citizen of Cordova, Tennessee.

71. When Plaintiff Hatfield became a patient of Upstream, Defendants required that she provide substantial amounts of her PII and PHI.

72. On or about September 15, 2023, Plaintiff Hatfield received a letter which told her that her PII and PHI had been impacted during the Data Breach. The notice letter informed her that the PII stolen included her name, social security number, medical billing information, medical record number, patient account number, and treatment information.

73. Plaintiff Hatfield suffered, and continues to suffer from, actual and imminent identity theft and misuse of her PII/PHI as a direct and/or proximate result of Upstream's actions and inactions.

74. Subsequent to the Data Breach, and in addition to the injuries and damages alleged herein, Plaintiff Hatfield has experienced actual fraudulent credit card applications on at least three occasions. In addition, Plaintiff Hatfield has received medical bills for services she did not actually receive. This fraudulent activity has caused Ms. Hatfield to spend a considerable amount of time combatting this fraud, in addition to causing her a significant amount of anxiety, and she is deeply worried about her identity being stolen as a result of the Data Breach.

75. Upstream's conduct, which allowed the Data Breach to occur, caused Plaintiff Hatfield significant injuries and harm, including but not limited to, the following—Ms. Hatfield immediately devoted (and must continue to devote) time, energy, and money to: closely monitor

her medical statements, bills, records, and credit and financial accounts; change login and password information on any sensitive account even more frequently than she already does; more carefully screen and scrutinize phone calls, emails, and other communications to ensure that she is not being targeted in a social engineering or spear phishing attack; search for suitable identity theft protection and credit monitoring services and paying for such services to protect herself; and place fraud alerts and/or credit freezes on her credit file. Plaintiff Hatfield has taken or will be forced to take these measures in order to mitigate her potential damages that are fairly traceable to the Data Breach.

76. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, in addition to the increased, imminent, and substantial risk of a future data breach and harm, Plaintiff Hatfield will need to maintain these heightened measures for years, and possibly her entire life.

77. Plaintiff Hatfield greatly values her privacy, especially while receiving medical services. She would not have obtained medical services from Upstream, or paid the amount she did to receive such, had she known that Upstream would negligently fail to adequately protect her PII/PHI. Indeed, Plaintiff Hatfield paid Upstream for medical care with the expectation that Upstream would keep her PII/PHI secure and inaccessible from unauthorized parties, as promised by Upstream.

78. Plaintiff Hatfield is also at a continued imminent and substantial risk of harm because her PII/PHI remains in Upstream systems, which have already been shown to be susceptible to compromise and attack and are subject to an increased and imminent future attack.

79. As a result of the Data Breach, and in addition to the time Plaintiff Hatfield has spent and anticipates spending to mitigate the impact of the Data Breach on his life, Ms. Hatfield

also suffered emotional distress from the public release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure. The emotional distress she experienced, and will continue to experience, includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing her PII and PHI for the purposes of identity theft and fraud.

80. Additionally, Plaintiff Hatfield has suffered damage to and diminution in the value of her highly sensitive and confidential PII/PHI—a form of property that she provided and entrusted to Upstream, and which was compromised as a result of the Data Breach Upstream failed to prevent. Plaintiff Hatfield has also suffered a violation of her privacy rights as a result of Upstream's unauthorized disclosure of her PHI/PII.

81. The free credit monitoring and identity restoration services offered by Upstream after the Data Breach were and continue to be ineffective because these services would have shared Ms. Hatfield's information with third parties and could not guarantee complete privacy of her sensitive information.

82. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Hatfield otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Hatfield lost was spent at Upstream's direction. Indeed, in the notice letter Plaintiff Hatfield received, Upstream directed her to spend time mitigating her losses by reviewing her accounts and credit reports for unauthorized activity.

83. Plaintiff Hatfield plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

Plaintiff Yashvantsinh Jhala

84. Plaintiff Jhala is and has been, at all relevant times, a resident and citizen of Madison County, Alabama.

85. Plaintiff Jhala became a patient of Upstream in or around September 2022.

86. On or about September 2023, Plaintiff Jhala received a letter which told him that his PII and PHI had been impacted during the Data Breach. The notice letter informed him that the PII stolen included his name, social security number, medical billing information, medical record number, patient account number, and treatment information.

87. Plaintiff Jhala suffered, and continues to suffer from, actual and imminent identity theft and misuse of her PII/PHI as a direct and/or proximate result of Upstream's actions and inactions.

88. Subsequent to the Data Breach, and in addition to the injuries and damages alleged herein, Plaintiff Jhala has discovered his emails and passwords on the dark web. In addition, Plaintiff Jhala has been denied credit subsequent to the Data Breach. This has caused Plaintiff Jhala to spend a considerable amount of time combatting this fraud, in addition to causing him a significant amount of anxiety, and he is deeply worried about his identity being stolen as a result of the Data Breach.

89. Upstream's conduct, which allowed the Data Breach to occur, caused Plaintiff Jhala significant injuries and harm, including but not limited to, the following—Mr. Jhala immediately devoted (and must continue to devote) time, energy, and money to: closely monitor his medical statements, bills, records, and credit and financial accounts; change login and password information on any sensitive account even more frequently than he already does; more carefully screen and scrutinize phone calls, emails, and other communications to ensure that he is not being targeted in a social engineering or spear phishing attack; search for suitable identity theft protection

and credit monitoring services and paying for such services to protect himself; and place fraud alerts and/or credit freezes on his credit file. Plaintiff Jhala has taken or will be forced to take these measures in order to mitigate his potential damages that are fairly traceable to the Data Breach.

90. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, in addition to the increased, imminent, and substantial risk of a future data breach and harm, Plaintiff Jhala will need to maintain these heightened measures for years, and possibly his entire life.

91. Plaintiff Jhala greatly values his privacy, especially while receiving medical services. He would not have obtained medical services from Upstream, or paid the amount he did to receive such, had he known that Upstream would negligently fail to adequately protect his PII/PHI. Indeed, Plaintiff Jhala paid Upstream for medical care with the expectation that Upstream would keep his PII/PHI secure and inaccessible from unauthorized parties, as promised by Upstream.

92. Plaintiff Jhala is also at a continued imminent and substantial risk of harm because his PII/PHI remains in Upstream systems, which have already been shown to be susceptible to compromise and attack and are subject to an increased and imminent future attack.

93. As a result of the Data Breach, and in addition to the time Plaintiff Jhala has spent and anticipates spending to mitigate the impact of the Data Breach on his life, he also suffered emotional distress from the public release of his PII and PHI, which he believed would be protected from unauthorized access and disclosure. The emotional distress he experienced, and will continue to experience, includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing his PII and PHI for the purposes of identity theft and fraud.

94. Additionally, Plaintiff Jhala has suffered damage to and diminution in the value of

his highly sensitive and confidential PII/PHI—a form of property that he provided and entrusted to Upstream, and which was compromised as a result of the Data Breach Upstream failed to prevent. Plaintiff Jhala has also suffered a violation of his privacy rights as a result of Upstream's unauthorized disclosure of his PHI/PII.

95. The free credit monitoring and identity restoration services offered by Upstream after the Data Breach were and continue to be ineffective because these services would have shared Plaintiff Jhala's information with third parties and could not guarantee complete privacy of his sensitive information.

96. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Jhala otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Jhala lost was spent at Upstream's direction. Indeed, in the notice letter Plaintiff Jhala received, Upstream directed him to spend time mitigating his losses by reviewing his accounts and credit reports for unauthorized activity.

97. Plaintiff Jhala plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

Plaintiff Dale Stark

98. Plaintiff Dale Stark is and has been, at all relevant times, a resident and citizen of Raceland, Louisiana.

99. Plaintiff Stark is a former patient of Upstream.

100. When Plaintiff Stark became a patient, Defendants required that he provide it with substantial amounts of his PII and PHI.

101. On or about September 15, 2023, Plaintiff Stark received a letter which told him

that his PII and PHI had been impacted during the Data Breach. The notice letter informed him that the PII stolen included his name, social security information, medical billing information, medical record number, patient account number, and treatment information.

102. Plaintiff Stark suffered, and continues to suffer from, actual and imminent identity theft and misuse of her PII/PHI as a direct and/or proximate result of Upstream's actions and inactions.

103. Subsequent to the Data Breach, and in addition to the injuries and damages alleged herein, Plaintiff Stark experienced fraudulent charges to his debit and/or credit cards. In addition, Plaintiff Stark has had unauthorized loans and debit cards opened and/or applied for in his name following the Data Breach. This has caused Plaintiff Stark to spend a considerable amount of time combatting this fraud, in addition to causing him a significant amount of anxiety, and he is deeply worried about his identity being stolen as a result of the Data Breach.

104. Upstream's conduct, which allowed the Data Breach to occur, caused Plaintiff Stark significant injuries and harm, including but not limited to, the following—Mr. Stark immediately devoted (and must continue to devote) time, energy, and money to: closely monitor his medical statements, bills, records, and credit and financial accounts; change login and password information on any sensitive account even more frequently than he already does; more carefully screen and scrutinize phone calls, emails, and other communications to ensure that he is not being targeted in a social engineering or spear phishing attack; search for suitable identity theft protection and credit monitoring services and paying for such services to protect himself; and place fraud alerts and/or credit freezes on his credit file. Plaintiff Stark has taken or will be forced to take these measures in order to mitigate his potential damages that are fairly traceable to the Data Breach.

105. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed

information has been fully recovered or contained against future misuse. For this reason, in addition to the increased, imminent, and substantial risk of a future data breach and harm, Plaintiff Stark will need to maintain these heightened measures for years, and possibly his entire life.

106. Plaintiff Stark greatly values his privacy, especially while receiving medical services. He would not have obtained medical services from Upstream, or paid the amount he did to receive such, had he known that Upstream would negligently fail to adequately protect his PII/PHI. Indeed, Plaintiff Stark paid Upstream for medical care with the expectation that Upstream would keep his PII/PHI secure and inaccessible from unauthorized parties, as promised by Upstream.

107. Plaintiff Stark is also at a continued imminent and substantial risk of harm because his PII/PHI remains in Upstream systems, which have already been shown to be susceptible to compromise and attack and are subject to an increased and imminent future attack.

108. As a result of the Data Breach, and in addition to the time Plaintiff Stark has spent and anticipates spending to mitigate the impact of the Data Breach on his life, he also suffered emotional distress from the public release of his PII and PHI, which he believed would be protected from unauthorized access and disclosure. The emotional distress he experienced, and will continue to experience, includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing his PII and PHI for the purposes of identity theft and fraud.

109. Additionally, Plaintiff Stark has suffered damage to and diminution in the value of his highly sensitive and confidential PII/PHI—a form of property that he provided and entrusted to Upstream, and which was compromised as a result of the Data Breach Upstream failed to prevent. Plaintiff Stark has also suffered a violation of his privacy rights as a result of Upstream's unauthorized disclosure of his PHI/PII.

110. The free credit monitoring and identity restoration services offered by Upstream after the Data Breach were and continue to be ineffective because these services would have shared Plaintiff Stark's information with third parties and could not guarantee complete privacy of his sensitive information.

111. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Stark otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Stark lost was spent at Upstream's direction. Indeed, in the notice letter Plaintiff Stark received, Upstream directed him to spend time mitigating his losses by reviewing his accounts and credit reports for unauthorized activity.

112. Plaintiff Stark plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

Plaintiff Adam Runk

113. Mr. Runk is an adult resident of Lewistown, Pennsylvania, a Patient of Drayer Physical Therapy Institute, a part of the Upstream Rehab Family of Care, and has suffered and will continue to suffer injuries and damages as set forth below.

114. Mr. Runk received medical treatment at Drayer in Lewistown, Pennsylvania in December 2021.

115. Mr. Runk suffered, and continues to suffer from, actual and imminent identity theft and misuse of his PII/PHI as a direct and/or proximate result of Upstream's actions and inactions.

116. Subsequent to the Data Breach, and in addition to the additional injuries and damages alleged herein, Plaintiff Runk has had a fraudulent charge of approximately $20 placed

on his account. To address this fraudulent activity, Mr. Runk has placed a freeze on his credit card. This fraudulent activity has caused Mr. Runk to spend a considerable amount of time combatting this fraud, in addition to causing him a significant amount of anxiety, and he is deeply worried about his identity being stolen as a result of the Data Breach.

117. Upstream's conduct, which allowed the Data Breach to occur, caused Plaintiff Runk significant injuries and harm, including but not limited to, the following—Mr. Runk immediately devoted (and must continue to devote) time, energy, and money to: closely monitor his medical statements, bills, records, and credit and financial accounts; change login and password information on any sensitive account even more frequently than he already does; more carefully screen and scrutinize phone calls, emails, and other communications to ensure that he is not being targeted in a social engineering or spear phishing attack; search for suitable identity theft protection and credit monitoring services and paying for such services to protect himself; and place fraud alerts and/or credit freezes on his credit file. Mr. Runk has taken or will be forced to take these measures in order to mitigate his potential damages that are fairly traceable to the Data Breach.

118. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, in addition to the increased, imminent, and substantial risk of a future data breach and harm, Mr. Runk will need to maintain these heightened measures for years, and possibly his entire life.

119. Mr. Runk greatly values his privacy, especially while receiving medical services. He would not have obtained medical services from Upstream, or paid the amount he did to receive such, had he known that Upstream would negligently fail to adequately protect his PII/PHI. Indeed, Mr. Runk paid Upstream for medical care with the expectation that Upstream would keep his PII/PHI secure and inaccessible from unauthorized parties, as promised by Upstream.

120. Mr. Runk is also at a continued imminent and substantial risk of harm because his PII/PHI remains in Upstream systems, which have already been shown to be susceptible to compromise and attack and are subject to an increased and imminent future attack.

121. As a result of the Data Breach, and in addition to the time Mr. Runk has spent and anticipates spending to mitigate the impact of the Data Breach on his life, Mr. Runk also suffered emotional distress from the public release of his PII and PHI, which he believed would be protected from unauthorized access and disclosure. The emotional distress he experienced, and will continue to experience, includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing their PII and PHI for the purposes of identity theft and fraud.

122. Additionally, Mr. Runk has suffered damage to and diminution in the value of his highly sensitive and confidential PII/PHI—a form of property that Mr. Runk provided and entrusted to Upstream, and which was compromised as a result of the Data Breach Upstream failed to prevent. Mr. Runk has also suffered a violation of his privacy rights as a result of Upstream's unauthorized disclosure of his PHI/PII.

123. The free credit monitoring and identity restoration services offered by Upstream after the Data Breach were and continue to be ineffective because these services would have shared Mr. Runk's information with third parties and could not guarantee complete privacy of his sensitive information.

Plaintiff Lisa Kenny

124. Plaintiff Kenny is an adult resident of Villa Rica, Georgia, a Patient of BenchMark Physical Therapy, a part of the Upstream Rehabilitation Family of Care, and has suffered and will continue to suffer injuries and damages as set forth below.

125. Plaintiff Kenny is a citizen of Georgia and brings this action in her individual

capacity and on behalf of all others similarly situated. Plaintiff Kenny has resided in the state of Georgia for nearly 56 years and owns a home in Villa Rica, Georgia. Plaintiff Kenny intends to remain in Georgia indefinitely.

126. Plaintiff Kenny received medical treatment at BenchMark in Villa Rica, Georgia in October and November of 2021.

127. Plaintiff Kenny suffered, and continues to suffer from, actual and imminent identity theft and misuse of her PII/PHI as a direct and/or proximate result of Upstream's actions and inactions.

128. Subsequent to the Data Breach, and in addition to the additional injuries and damages alleged herein, on October 17, 2023, Plaintiff Kenny was notified by JPMorgan Chase of an unauthorized credit card application submitted in her name. To address this fraudulent activity, Plaintiff Kenny has reached out to the bank and the credit monitoring service Experian. This fraudulent activity has caused Plaintiff Kenny to spend a considerable amount of time combatting this fraud, in addition to causing her a significant amount of anxiety, and she is deeply worried about her identity being stolen as a result of the Data Breach.

129. In In addition to this unauthorized activity, Plaintiff Kenny has experienced an acute increase in spam and phishing emails to her work account which has caused her to spend a considerable amount of time reviewing and deleting emails, telephone calls and voicemails.

130. Upstream's conduct, which allowed the Data Breach to occur, caused Plaintiff Kenny significant injuries and harm, including but not limited to, the following— Plaintiff Kenny immediately devoted (and must continue to devote) time, energy, and money to: closely monitor her medical statements, bills, records, and credit and financial accounts; change login and password information on any sensitive account even more frequently than she already does; more

carefully screen and scrutinize phone calls, emails, and other communications to ensure that she is not being targeted in a social engineering or spear phishing attack; search for suitable identity theft protection and credit monitoring services and paying for such services to protect herself; and place fraud alerts and/or credit freezes on her credit file. Plaintiff Kenny has taken or will be forced to take these measures in order to mitigate her potential damages that are fairly traceable to the Data Breach.

131. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, in addition to the increased, imminent, and substantial risk of a future data breach and harm, Plaintiff Kenny will need to maintain these heightened measures for years, and possibly her entire life.

132. Plaintiff Kenny greatly values her privacy, especially while receiving medical services. She would not have obtained medical services from Upstream, or paid the amount she did to receive such, had she known that Upstream would negligently fail to adequately protect her PII/PHI. Indeed, Plaintiff Kenny paid Upstream for medical care with the expectation that Upstream would keep her PII/PHI secure and inaccessible from unauthorized parties, as promised by Upstream.

133. Plaintiff Kenny is also at a continued imminent and substantial risk of harm because her PII/PHI remains in Upstream systems, which have already been shown to be susceptible to compromise and attack and are subject to an increased and imminent future attack.

134. As a result of the Data Breach, and in addition to the time Plaintiff Kenny has spent and anticipates spending to mitigate the impact of the Data Breach on her life, Plaintiff Kenny also suffered emotional distress from the public release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure. The emotional distress she

experienced, and will continue to experience, includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing their PII and PHI for the purposes of identity theft and fraud.

135. Additionally, Plaintiff Kenny has suffered damage to and diminution in the value of her highly sensitive and confidential PII/PHI—a form of property that Plaintiff Kenny provided and entrusted to Upstream, and which was compromised as a result of the Data Breach Upstream failed to prevent. Plaintiff Kenny has also suffered a violation of her privacy rights as a result of Upstream's unauthorized disclosure of her PHI/PII.

136. The free credit monitoring and identity restoration services offered by Upstream after the Data Breach were and continue to be ineffective because these services would have shared Plaintiff Kenny's information with third parties and could not guarantee complete privacy of her sensitive information.

137. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Kenny otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff lost was spent at Upstream's direction. Indeed, in the notice letter Plaintiff received, Upstream directed Plaintiff to spend time by reviewing her accounts and credit reports for unauthorized activity.

Plaintiff Judy Young

138. Plaintiff Judy Young is and has been, at all relevant times, a resident and citizen of Anniston, Alabama.

139. When Plaintiff Young became a patient, Defendants required that she provide substantial amounts of her PII and PHI.

140. On or about September 15, 2023, Plaintiff Young received a notice letter which

told her that her PII and PHI had been impacted during the Data Breach. The notice letter informed her that the information stolen included her name, medical record number, health insurance information, patient account number, and treatment information.

141. The notice letter offered Plaintiff Young only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Young has already experienced (and will continue to experience) a substantial, continuous, and increased risk of identity theft, including but not limited to, potential identify theft and medical fraud.

142. To the best of her knowledge, other than Defendants' Data Breach Plaintiff Young's PII and PHI have not been included in any other data breaches or otherwise been accessed without authorization.

143. In In addition, Plaintiff Young has suffered actual injury in the form of time spent monitoring her accounts for fraud and dealing with and attempting to mitigate the devastating impact the Data Breach has already had on her life, including but not limited to, the actual and increased risk of fraud he has experienced resulting from the Data Breach. Defendants specifically instructed Plaintiff Young to devote time and effort responding to the Data Breach.

144. Plaintiff Young would not have provided her PII and PHI to Defendants had Defendants timely disclosed that its systems lacked adequate computer and data security practices to safeguard its patients' personal and health information from theft, and that those systems were subject to multiple data breaches.

Defendants Upstream Rehabilitation, Inc. and Upstream RollCo, LLC

145. Defendant Upstream Rehabilitation, Inc. is a corporation that has its principal place of business in Jefferson County, Alabama located at 1200 Corporate Dr. Suite 400, Birmingham, Alabama 35242. Additionally, Upstream is a healthcare entity registered and

qualified to do business in Alabama, and was doing business in Jefferson County, Alabama at all times materially relevant hereto.

146. Defendant Upstream RollCo, LLC is a Delaware limited liability company that has its principal place of business in Jefferson County, Alabama located at 1200 Corporate Dr., Suite 400, Birmingham, Alabama 35242. Upon information and belief, Upstream RollCo, LLC operates under the trade name Upstream Rehabilitation and the membership of Upstream RollCo, LLC is comprised of members who are either Alabama resident citizens or corporations.

147. Whenever reference in this Complaint is made to any act or transaction of Upstream, such allocations shall be deemed to mean that the principals, officers, employees, agents, and/or representatives of Upstream committed, knew of, performed, authorized, ratified and/or directed such transaction on behalf of Upstream while actively engaged in the scope of their duties.

BACKGROUND FACTS

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

148. In the regular course of its business, Upstream acquires, collects, stores and maintains possession, custody, and control of a wide variety and massive amount of information of Plaintiffs' and Class Members' personal and confidential information, including: full names, addresses, telephone numbers, email addresses, dates of birth, Social Security numbers, Passport and Driver's License numbers, medical and treatment information, billing and claims information, health insurance information, financial account information, and/or credit and debit card information.

149. As a condition of engaging in health services, Upstream requires that its customers (patients) provide and entrust it with highly sensitive and confidential personal information.

150. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII/PHI, Upstream assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII/PHI from disclosure.

151. 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, relied on Upstream 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 sensitive information.

152. Upstream acknowledged its obligation to maintain the privacy of Patient PII/PHI entrusted to it by Plaintiffs and Class Members through its Notice of Privacy Practices. Upstream's Notice of Privacy Practices represents, inter alia, that it "is required by law to maintain the privacy of your health information."

153. Upstream stored Plaintiffs' and Class Members' PII/PHI, at a minimum, in an unprotected, unguarded, unsecured, and/or otherwise unreasonable location.

154. Upstream stored the Plaintiffs' and Class Members' PII/PHI in a location that had inadequate security to prevent unauthorized access.

155. Upstream's Notice states: "We encourage you to remain vigilant against incidents of theft and fraud by reviewing account statements and explanation of benefits and monitoring free credit reports for suspicious activity and to detect errors." [5]

Upstream's Data Breach

156. Beginning as early as January 24, 2023, an unauthorized third party accessed

[5] See https://consumer.sc.gov/sites/consumer/files/Documents/Security%20Breach%20Notices/UpstreamRollCoLLC.pdf (sample breach letter).

Upstream's networks, data systems, and/or servers.

157. Between January 24, 2023 through January 31, 2023, as well as February 3, 2023 through February 9, 2023, digital files containing Plaintiffs' and Class Members' unencrypted PII/PHI were accessed from Upstream's networks, data systems, and/or servers by unauthorized third parties.

158. Upstream finally discovered that between January 24, 2023 through January 31, 2023, as well as February 3, 2023 through February 9, 2023 an unauthorized third party gained access to its networks, data systems, and/or servers, including sensitive files containing Plaintiffs' and Class Members' PII/PHI. However, the detection of the unauthorized activity was ***days over*** unauthorized third parties accessed and exfiltrated Patient.

159. Thereafter, Upstream determined that an unauthorized third party not only accessed Plaintiffs' and Class Members' PII/PHI, but exfiltrated or removed data from its networks and servers.

160. On or about September 15, 2023, eight (8) months after discovering the Data Breach, Upstream finally informed Plaintiffs and Class Members of the Data Breach by mailing them the following Notice Letter. [6]

161. The Privacy Policy posted on Upstream's website reassures: "Upstream Rehabilitation is required by state and federal law to maintain the privacy of your Protected Health Information ("PHI") and to provide you with notice of our legal duties and privacy practices with respect to PHI. PHI includes the information and records we have about your health, and the health care services you receive in our facility. PHI is information that may identify you and that relates to your past, present, or future physical or mental health or condition and related health care

[6] *Notice Letter* attached hereto as **Exhibit A.**

services.[7]

162. Upstream's Letter to Plaintiffs and Class Members state that Upstream discovered the unauthorized access of its networks and servers and that a subsequent investigation determined that the third party was able to remove a copy of data from the network between January 24, 2023 through January 31, 2023, as well as February 3, 2023 through February 9, 2023.

163. Given the period of time during which unauthorized third parties had access to its files—and the multiple months between Upstream's discovery of the Data Breach and Upstream's public disclosure of it—the Plaintiffs' and Class Members' PII/PHI has likely been bought and sold several times on the robust international cyber black market while Upstream denied the Plaintiffs and Class Members any opportunity to take measures to protect their PII/PHI and privacy, which created an imminent and substantial risk of harm and identity theft that is ongoing.

164. Upstream's wrongful actions and/or inactions—to wit, failing to protect Plaintiffs' and Class Members' PII/PHI with which it was entrusted—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 Upstream's wrongful actions and/or inactions, Plaintiffs and Class Members have suffered, and will continue to suffer, injuries and damages including, without limitation: (i) an increased and imminent risk of substantial harm; (ii) the untimely and/or inadequate notification of the Data Breach; (iii) improper disclosure, dissemination and publication of their PII/PHI; (iv) criminal misuse of their PII/PHI; (v) identity theft; (vi) financial fraud; (vii) loss of privacy; (viii) 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; (ix)

[7] *See https://urpt.com/privacy-policy/ (last visited June 21, 2024).*

economic losses relating to the theft of their PII/PHI; (x) 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; (xi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (xii) stress, anxiety and emotional distress.

165. Notwithstanding Upstream's wrongful actions and/or inactions, Upstream has offered a mere one year of ineffective credit monitoring services, which is wholly inadequate and insufficient, given the trove of PII/PHI that has been taken and disseminated to the world.

166. As a result of Upstream's 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, confidential, and sensitive in nature and was left inadequately protected by Upstream.

167. Upstream's 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, imminent and substantial risk of identity theft and identity fraud that is fairly traceable to the Data Breach.

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

168. Identity theft occurs when a person's PII/PHI, such as the person's name, address, date of birth, Social Security number, billing and mailing addresses, phone number, email, credit card information, and health information is used without his or her permission to commit fraud or other crimes.[8]

169. 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

[8] *See* https://consumer.ftc.gov/articles/what-know-about-identity-theft#what_is (last visited November 28, 2023).

that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[9] Furthermore, "there is significant evidence demonstrating that technological 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]."[10]

170. The FTC estimates that the identities of as many as nine million Americans are stolen each year. *Id.*

171. As a direct and/or proximate result of the Data Breach, Plaintiffs and Class Members have been, and will continue to be, required to spend money and to take the time and effort to combat actual or suspected 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, reviewing, closing or modifying financial accounts, scrutinizing their credit reports and bank and credit accounts, and purchasing products to monitor their credit reports and financial accounts for unauthorized activity. Because Plaintiffs' and Class Members' PII/PHI were stolen and/or compromised, they also now face a significantly heightened and imminent risk of harm and identity theft.

172. Citizens of Alabama, like some of the members of the proposed class here, have suffered particularly severe losses from cybercrimes lately. A recent news article explained:

> According to the latest data on internet crimes compiled by the Federal Bureau of Investigation, Alabama saw the single-highest average of losses to cybercrime per victim in 2022. Research on the data published Friday by the online security company VPNpro found that ***victims of cybercrimes in Alabama lost, on average,***

---

[9] Protecting Consumer Privacy in an Era of Rapid Change FTC Report (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 November 28, 2023).

[10] *Id*., at 11–12.

$50,670 in 2022. A total of 4,893 victims were reported in Alabama that year for a combined loss of nearly $248,000,000.[11]

173. 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."[12]

174. 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 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."[13]

175. 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, which places Plaintiffs at an increased and imminent risk of further future harm. Moreover, unlike other PII/PHI, Social Security numbers are incredibly difficult to change, and their misuse can continue for years into

[11] *See* https://aldailynews.com/alabamians-see-highest-losses-to-cybercrime-in-nation-new-research-finds/ (last visited November 28, 2023) (emphasis added).

[12] *See* https://consumer.ftc.gov/articles/what-know-about-identity-theft#what_is (last visited November 28, 2023).

[13] *See* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited November 28, 2023).

the future.

176. Identity thieves 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 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."

177. 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 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.[14] Thus, a person whose PII/PHI has been stolen cannot obtain a new Social Security number until the damage has already been done.

178. Obtaining a new Social Security number, however, 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 a credit history.

[14] *See* https://consumer.ftc.gov/articles/do-you-need-new-social-security-number (last visited November 28, 2023).

179. Phone numbers are de facto identity documents, given the increasing reliance on using phone numbers as verification (i.e., two-factor authentication to access basic web pages.). A loss of a person's phone number can be as much of, if not more of, a risk than loss of a social security number—resulting in increased scam calls or loss of ability to access a web page.

180. As a direct and/or proximate result of Upstream's 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 not only already lost actual value but have been deprived, and will continue to be deprived, of the value of their PII/PHI.[15]

181. 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.[16] 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.

182. The Data Breach was a direct and/or proximate result of Upstream's 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 federal and state regulations and industry practices.

183. Upstream flagrantly disregarded and/or violated Plaintiffs' and Class Members'

---

[15] *See, e.g.,* John T. Soma, J. Zachary Courson, John Cadkin, *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); ABC News Report, http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986&page=2#.UGRgtq7yBR4 (last visited November 28, 2023).

[16] 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).

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 policies.

184. Upstream flagrantly disregarded and/or violated Plaintiffs' and Class Members' privacy rights, and have 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. Upstream's security deficiencies allowed unauthorized individuals to access, remove from its servers and networks, disclose, and/or compromise the PII/PHI over four-hundred thousand of its Patients—including Plaintiffs and Class Members.

185. Upstream's wrongful actions and/or inactions 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 Upstream's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and Class Members have incurred injuries and damages in the form of, *inter alia*: (i) an increased and imminent risk of future harm; (ii) the untimely and/or inadequate notification of the Data Breach; (iii) improper disclosure, dissemination and publication of their PII/PHI; (iv) criminal misuse of their PII/PHI; (v) identity theft; (vi) financial fraud; (vii) loss of privacy; (viii) 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; (iv) economic losses relating to the theft of their PII/PHI; (x) 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; (xi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (xii) stress, anxiety and emotional distress. Plaintiffs' and Class Members' damages were foreseeable by Upstream.

C. ***Healthcare Organizations are Known High Risk Targets of Cyber Attackers***

186. The risk of harm to Plaintiffs and Class Members from Upstream's failure to take precautionary measures was readily and clearly foreseeable. Not only was Upstream aware of the risks created by its inaction, but it was also in a unique position to know of the risk and prevent it.

187. Hospitals and healthcare organizations have become an attractive target of cyberattacks because they house a gold mine of sensitive, personally identifiable information for thousands of patients at any given time. From Social Security numbers and insurance policies to credit cards and emergency contacts' information, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.[17] As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to quickly regain access to their data."[18]

188. Healthcare records are also preferred targets of cyberattacks because those records include far more information than other targets of cyberattacks (such as bank account numbers), and it has been estimated that medical records are **fifty times more valuable** on the black market

[17] https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited November 28).
[18] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targetedransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited November 28, 2023).

than credit cards.[19]

189. As such, it has been reported that "[s]tolen healthcare records are the source of 95% of all identity theft[.]"[20] According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernible across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors, leveraging emails to compromise the integrity of their targets."[21]

190. Despite years of rising awareness of healthcare organizations' position as the preeminent target of cyberattacks, the healthcare industry continues to suffer more data breaches than any other industry. According to Identity Theft Resource Center ("ITRC"), the healthcare industry in 2022, for the third year in a row, led all other industries in the number of data breaches.[22] Additionally, "[h]ealthcare organizations represented 19 percent of the 1,802 breaches reported in the 2022 IRTC report."[23]

191. Indeed, cyberattacks against healthcare organizations have become so prevalent that the Federal Bureau of Investigation ("FBI") has specifically warned that industry of the threat it faces and has given it recommendations to protect against data breaches.[24]

192. Therefore, the prevalence of such attacks, and the attendant, increased, and

---

[19] *See* https://www.dmagazine.com/healthcare-business/2019/10/why-medical-data-is-50-times-more-valuable-than-a-credit-card/ (last visited November 28, 2023).
[20] *See* https://www.globenewswire.com/en/news-release/2022/03/31/2413675/0/en/Largest-Healthcare-Data-Breaches-Reported-in-February-2022-Confirms-Need-for-Network-Security-Based-on-Zero-Trust-Microsegmentation.html (last visited November 28, 2023).
[21] *See* https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited November 28, 2023).
[22] *See* https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final.pdf (last visited November 28, 2023).
[23] https://www.prnewswire.com/news-releases/healthcare-remains-top-target-in-2022-itrc-breach-report-301730483.html (last visited November 28, 2023).
[24] *See* https://www.aha.org/cybersecurity-government-intelligence-reports/2022-09-12-fbi-pin-tlp-white-unpatched-and-outdated (last visited November 28, 2023).

imminent risk of future attacks, was widely known to the public and anyone in the healthcare industry, including Upstream.

D. *Upstream's Conduct Violated HIPAA and Industry Standard Practices*

193. 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 Upstream left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

194. Upstream's Data Breach resulted from a combination of insufficiencies that indicate Upstream failed to comply with safeguards mandated by HIPAA regulations and industry standards. Upstream's 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', 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 Upstream creates, receives, maintains, and transmits 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 its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its 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).

195. Upstream is still in possession of Plaintiffs' PII/PHI and, without the injunctive relief requested herein, Plaintiffs and Class Members remain at substantial risk of having their PII/PHI stolen again in a future data breach due to Upstream's woefully inadequate data security and cybersecurity. Upstream has not invested the necessary resources into data security or cybersecurity, and another future data breach is imminent and likely to occur at any time.

196. The substantial risk of harm to Plaintiffs would be greatly reduced or eliminated by the injunctive relief requested herein, because the additional cybersecurity measures and policies would be capable of deterring would-be hackers and other cybersecurity threats—unlike Upstream current data security and cybersecurity measures, which have proven to be vulnerable to criminals.

197. The state of Alabama's public health department follows HIPAA guidance and requires medical providers to as well.

198. Upstream violated federal and state statutes and industry standards to better secure its information privacy practices following the breach, which further created an imminent and substantial risk of future harm and identity theft.

199. Upstream also violated industry standards by shifting liability from its business practices to patients to mitigate the damages caused by the Data Breach. Patients cannot be expected to understand how to best mitigate damages from Upstream's enterprise-wide cybersecurity breaches.

CLASS ACTION ALLEGATIONS

200. Pursuant to Rule 23 of the Alabama Rules of Civil Procedure, Plaintiffs bring this

class action on behalf of themselves and the following Nationwide Class of similarly situated individuals:

> **All individuals whose personal identifying information (PII) and personal health information (PHI) was exposed to unauthorized third parties as a result of the Data Breach discovered by Upstream.**

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

202. The putative Class is comprised of persons who are citizens of many different states, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

203. The rights of each Class Member were violated in a virtually identical manner as a result of Upstream's willful, reckless, negligent and/or wanton actions and/or inactions.

204. 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 Upstream willfully, recklessly, negligently and/or wantonly failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class Members' PII/PHI;

b. Whether Upstream was negligent or wanton in the manner in which it stored Plaintiffs' and Class Members' PII/PHI;

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

d. Whether Upstream breached its duty to exercise reasonable care in protecting and securing Plaintiffs' and Class Members' PII/PHI;

e. Whether Upstream was negligent in failing to secure Plaintiffs' and Class Members' PII/PHI;

f. Whether Upstream failure to comply with HIPAA constitutes negligence *per se*;

g. Whether Upstream's failure to comply with Section 5 of the Federal Trade Commission

Act (15 U.S.C. §45) constitutes negligence *per se*;

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

i. Whether Upstream breached its 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, Upstream invaded Plaintiffs' and Class Members' privacy;

k. Whether by publicly disclosing Plaintiffs' and Class Members' PII/PHI without authorization, Upstream breached the duty of confidence it owed to Plaintiffs and Class Members;

l. Whether by publicly disclosing Plaintiffs' and Class Members' PII/PHI without authorization, Upstream breached the fiduciary duties it owed to Plaintiffs and Class Members;

m. Whether Upstream was unjustly enriched when it took money from Plaintiffs and Class Members and failed to provide reasonable data security measures to protect Plaintiffs' and Class Members' PII/PHI;

n. Whether Plaintiffs and Class Members sustained damages as a result of Upstream's failure to secure and protect their PII/PHI; and,

o. Whether injunctive relief is necessary to ensure Upstream implements reasonable security measures to protect the PII/PHI of Plaintiffs and the Class Members against any future data breaches by Upstream.

205. Plaintiffs' claims are typical of Class Members' claims in that Plaintiffs' claims and Class Members' claims all arise from Upstream's failure to properly secure, safeguard and protect Plaintiffs' and Class Members' PII/PHI and the resulting Data Breach.

206. 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 class action litigators and intend to vigorously prosecute this action on behalf of Plaintiffs and Class Members.

207. 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 Upstream's wrongful actions and/or inactions. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Upstream's failure to secure, safeguard and protect Plaintiffs' and Class Members' PII/PHI.

208. 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.

209. Class certification also is appropriate pursuant to ALA. R. CIV. P. 23(b)(2) because Upstream has acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the putative class as a whole.

210. 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

211. Plaintiffs re-adopt and re-allege the factual allegations contained in the preceding paragraphs, and further allege as follows.

212. Upstream had a duty to exercise reasonable care in obtaining, using, retaining, securing, safeguarding, and protecting Plaintiffs' and Class Members' PII/PHI in its possession, including implementing federal, state, and industry standard security procedures sufficient to reasonably protect PII/PHI from unauthorized third parties.

213. Upstream owed a duty of care to Plaintiffs' and Class Members' because it was reasonably foreseeable that its failure to adequately safeguard the PII/PHI in accordance with federal, state, and industry standards for data security would result in the compromise of that

PII/PHI and failing to safeguard the private information would be a conscious disregard and would put the Plaintiffs' and Class Members' at an increased, imminent risk of substantial harm and identity theft.

214. Upstream negligently and/or wantonly violated its duty by failing to exercise reasonable care in securing, safeguarding, and protecting Plaintiffs' and Class Members' PII/PHI (as set forth in detail above).

215. Upstream acted with conscious disregard for Class Members' PII/PHI because Upstream was aware of other data healthcare data breaches prior to this Data Breach, yet Upstream chose to do nothing to strengthen the cybersecurity to protect Plaintiffs' data.

216. After the previous data breaches, Upstream executives and employees knew that their decision not to invest additional resources into Upstream's cybersecurity left the Plaintiffs' PII/PHI at risk of being accessed and/or exfiltrated by cybercriminals.

217. Upstream's conduct set forth herein was so reckless and so charged with indifference and conscious disregard 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.

218. It was reasonably foreseeable that Upstream's 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.

219. Plaintiffs and the Class Members have suffered (and continue to suffer) actual, injuries-in-fact, and damages as a direct and/or proximate result of Upstream's failure to secure, safeguard 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.

220. Upstream's wrongful actions and/or inaction (as described above) constituted negligence and/or wantonness at common law.

COUNT II
NEGLIGENCE *PER SE*

221. Plaintiffs re-adopt and re-allege the factual allegations contained in the preceding paragraphs, and further allege as follows.

222. 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 Upstream and with which Upstream was obligated to comply at all relevant times hereto.

223. Upstream violated these duties by failing to secure, 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.

224. Subsection 8-38-3(a) of the Alabama Data Breach Notification Act of 2018 imposes a clear duty on healthcare entities like Upstream 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."

225. Upstream 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 PII/PHI against a breach of security.

226. 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 Plaintiffs 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 patient's individually identifiable health information.

227. Upstream was 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 Upstream's duty.

228. Upstream violated Section 5 of the FTC Act by failing to maintain reasonable and appropriate data security for its Patients' PII/PHI.

229. 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.

230. Plaintiffs and Class Members, as owners of the sensitive personally identifying information that Upstream 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.

231. Subsection 8-38-5(b) of the Alabama Data Breach Notification Act of 2018 further imposes a clear duty on healthcare entities like Upstream 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."

232. Upstream breached its duty to promptly notify Plaintiffs and Class Members by failing to send out notification letters until approximately 60 days after it purportedly discovered the Data Breach.

233. 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.

234. As a direct and proximate result of Upstream's violation of HIPAA's Privacy Rule, the FTC Act, and the Alabama Data Breach Notification Act of 2018, the Plaintiffs and Class Members were damaged in the form of, without limitation, loss of time monitoring credit reports and financial accounts and placing credit freezes, 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 AND/OR IMPLIED CONTRACT

235. Plaintiffs re-adopt and re-allege the factual allegations contained in the preceding paragraphs, and further allege as follows.

236. Upstream offered to provide goods and services to Plaintiffs' and Class Members' in exchange for payment and required Plaintiffs and Class Members' to provide Upstream with their PII/PHI in order to receive such goods and services.

237. Upstream had a written agreement and understanding with the Plaintiffs and the Class Members as set forth in Upstream Notice of Privacy Practices that Upstream would not disclose Plaintiffs' or the Class Members' confidential information in a manner not authorized by applicable law or industry standards.

238. Upstream'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.

239. Further, Alabama law imposes on physicians and health care professionals an implied contract of confidentiality that is breached by the unauthorized release of medical information, and Upstream breached those implied contracts with Plaintiffs and Class Members when it released their PII/PHI to unauthorized third parties.

240. Upstream materially breached its contracts with the Plaintiffs and the Class Members by failing to secure, safeguard and protect Plaintiffs' and the Class Members' PII/PHI such that an unauthorized disclosure of Plaintiffs' and the Class Members' PII/PHI occurred.

241. As a direct and proximate result of Upstream's breach of its contracts with the Plaintiffs and the Class Members, Plaintiffs and the Class Members have been, and continue to be, damaged in an amount to be proven at trial.

242. 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
BREACH OF FIDUCIARY DUTY

243. Plaintiffs re-adopt and re-allege the factual allegations contained in the preceding paragraphs, and further allege as follows.

244. Upstream had a fiduciary duty to secure, safeguard and protect private patient information, which included Plaintiff and Class Members.

245. Upstream became a fiduciary over Plaintiffs' and Class Members' by its undertaking and guardianship of the PII/PHI, to act primarily for the benefit of Plaintiffs' and Class Members', (1) for the safeguarding of Plaintiffs and Class Members' PII/PHI; (2) to timely notify Plaintiffs' and Class Members' of a data breach and disclosure; and (3) to maintain complete and accurate records of what patient information (and where) Upstream did and does store.

246. Upstream breached this duty when it did not protect Plaintiff and Class Members private information.

247. Upstream breached this duty when it did not provide adequate and timely notification of the Data Breach to Plaintiff and Class Members.

248. Upstream breached its fiduciary duty when it violated 45 C.F.R. § 164.306(a)(1) by failing to ensure the confidentiality and integrity of Plaintiff and Class Member's protected and electronic health information (i.e., PHI) that Upstream created, received, maintained, and transmitted.

249. Upstream breached its fiduciary duty when it violated 45 C.F.R. § 164.312(a)(1) by failing to implement technical policies and procedures for its electronic information systems housing private information.

250. Upstream breached its fiduciary duty when it violated 45 C.F.R. § 164.308(a)(1) by failing to implement policies and procedures to prevent, detect, contain, and correct security violations.

251. Upstream breached its fiduciary duty when it violated 45 C.F.R. § 164.308(a)(6)(ii) by failing to mitigate, to the extent practicable, harmful effects of security incidents that were known to Upstream.

252. Upstream breached its fiduciary duty when it violated 45 C.F.R. § 164.306(a)(2) by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic private information, or PII/PHI.

253. Upstream breached its fiduciary duty when it violated 45 C.F.R. § 106.308(a)(6)(ii) by failing to mitigate harmful effects of security incidents known to Upstream.

254. Upstream breached its fiduciary duty when it violated 45 C.F.R. § 164.306(a)(2) by failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic private information.

255. Upstream violated 45 C.F.R. § 164.306(a)(3) when it failed to protect against reasonably anticipated uses or disclosures.

256. Upstream breached its fiduciary duty when it violated 45 C.F.R. § 164.530(b), and 45 C.F.R. § 164.308(a)(5) by failing to ensure that its workforce complied with HIPAA and failing to provide adequate training to their workforce.

257. Upstream breached its fiduciary duty when it violated 45 C.F.R. § 164.502 by impermissibly and improperly using and disclosing private information that remains accessible to unauthorized people.

258. Upstream breached its fiduciary duty when it violated 45 C.F.R. § 164.530(c) by failing to design, implement, and enforce policies and procedures to establish a physical administrative safeguard to protect private information, such as PII/PHI.

259. Plaintiff and Class Members face injuries as a direct and proximate result of

Upstream's breaches of its fiduciary duties. These injuries include, but are not limited to:

a. Loss of control over private information;

b. Compromise of private information;

c. Lost opportunity costs associated with time spent to protect themselves and mitigating harm;

d. Continued risk that Plaintiff and Class Members private information could be stolen again;

e. Future costs associated with time spent protecting themselves from future harm;

f. Diminished value of Upstream's services;

g. Diminished value of private information; and

h. Anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
BREACH OF CONFIDENCE

260. Plaintiffs re-adopt and re-allege the factual allegations contained in the preceding paragraphs, and further allege as follows.

261. At all times during Plaintiffs' and Class Members' interactions with Upstream, Upstream was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' private information that Plaintiffs and Class Members provided to Upstream.

262. As alleged herein and above, Upstream's relationship with Plaintiffs and Class Members was governed by expectations that Plaintiffs' and Class Members' private information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

263. Plaintiffs and Class Members provided their respective private information to

Upstream with the explicit and implicit understandings that Upstream would protect and not permit the private information to be disseminated to any unauthorized parties.

264. Plaintiffs and Class Members also provided their respective private information to Upstream with the explicit and implicit understanding that Upstream would take precautions to protect that private information from unauthorized disclosure, such as following basic principles of information security practices.

265. Due to Upstream's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiffs' and Class Members' private information, Plaintiffs' and Class Members' private information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

266. But for Upstream's disclosure of Plaintiffs' and Class members' private information in violation of the parties' understanding of confidence, their private information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Upstream's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' private information, as well as the resulting damages.

267. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Upstream's unauthorized disclosure of Plaintiffs' and Class Members' private information. Upstream knew or should have known its security systems were insufficient to protect the private information that is coveted by thieves worldwide. Upstream also failed to observe industry standard information security practices.

268. As a direct and proximate cause of Upstream's conduct, Plaintiffs and Class Members suffered damages as alleged above.

COUNT VI
UNJUST ENRICHMENT

269. Plaintiffs re-adopt and re-allege the factual allegations contained in the preceding paragraphs, and further allege as follows.

270. Plaintiffs bring this claim in the alternative to their Implied Contract claim.

271. Plaintiffs and Class Members conferred a monetary benefit on Upstream. Specifically, Plaintiffs and Class Members purchased goods and services from Upstream and provided Upstream with their private information. In exchange, Plaintiffs and Class Members should have received from Upstream the goods and services that were the subject of the transaction and should have been entitled to have Upstream protect their private information with adequate data security.

272. Upstream knew that Plaintiffs and Class Members conferred a benefit on Upstream and have accepted or retained that benefit. Upstream profited from Plaintiffs' purchases and used Plaintiffs' and Class Members' private information for business purposes.

273. Upstream failed to secure Plaintiffs' and Class Members' private information and, therefore, did not fully compensate Plaintiffs and Class Members for the value that their private information provided.

274. Upstream acquired the private information through inequitable means as it failed to disclose the inadequate security practices previously alleged.

275. If Plaintiffs and Class Members knew that Upstream would not secure their private information using adequate security, they would have made alternative healthcare choices that excluded Upstream.

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

277. Under the circumstances, it would be unjust for Upstream to be permitted to retain

any of the benefits that Plaintiffs and Class Members conferred on it.

278. Upstream should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Upstream should be compelled to refund the amounts that Plaintiffs and Class Members overpaid.

RELIEF REQUESTED

279. Plaintiffs re-adopt and re-allege the factual allegations contained in the preceding paragraphs, and further allege as follows.

280. **DAMAGES.** As a direct and/or proximate result of Upstream's wrongful actions and/or inactions (as described above), Plaintiffs and Class Members suffered (and continue to suffer) 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) loss of privacy; (v) suspected and/or actual identity theft /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 suspected and/or actual 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 Upstream.

281. **EXEMPLARY DAMAGES.** Plaintiffs and Class Members also are entitled to exemplary damages to punish Upstream and to deter such wrongful conduct in the future.

282. **INJUNCTIVE RELIEF.** Plaintiffs and Class Members also are entitled to

injunctive relief in the form of, without limitation, requiring Upstream to, *inter alia*, (i) immediately disclose to Plaintiffs and Class Members the precise nature and all details known to Upstream regarding the Data Breach, (ii) immediately secure the PII/PHI of its past, present, and future patients, (iii) implement the above-referenced proactive policies and procedures in order to secure and protect its patients' PII/PHI and be in a position to immediately notify them about any future data breaches, (iv) submit to periodic compliance audits by a third party regarding the implementation of and compliance with such policies and procedures, (v) submit to periodic compliance audits by a third party regarding the security of its patients' PII/PHI within its possession, custody and control, (vi) implement training for its personnel on new or modified security procedures through education programs, policies and tests, and (vii) pay for, not less than three years, identity theft and credit monitoring services for Plaintiffs and Class Members. Plaintiffs have standing to pursue injunctive relief. *See* Ala. Const. of 2022, art. I, section 10. ("That no person shall be barred from prosecuting or defending before any tribunal in this state, by himself or counsel, any civil cause to which he is a party.")

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, respectfully request that (i) Upstream be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiffs be designated the Class Representatives, and (iv) Plaintiffs' counsel be appointed as Class Counsel. Plaintiffs, on behalf of themselves and Class Members, further request that upon final trial or hearing, judgment be awarded against Upstream, in favor of Plaintiffs and the Class Members, for:

i. actual damages, consequential damages, and/or nominal damages (as described above) in an amount to be determined by the trier of fact;

ii. exemplary damages;

iii. injunctive relief as set forth above;

iv. pre- and post-judgment interest at the highest applicable legal rates;

v. costs of suit and attorneys' fees; and,

vi. such other and further relief that this Court deems just and proper.

JURY DEMAND

Plaintiffs respectfully demand a trial by jury on all claims and causes of action so triable.

Dated: June 26, 2024

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

Hirlye R. "Ryan" Lutz, III (LUT005)
F. Jerome Tapley (TAP006)
Hunter Phares (PHA007)
CORY WATSON, P.C.
2131 Magnolia Avenue South
Birmingham, AL 35205
Tel: (205) 328-2200
Fax: (205) 324-7896
Email: rlutz@corywatson.com
Email: jtapley@corywatson.com
Email: hphares@corywatson.com

Daniel Srourian, Esq. (*pro hac vice forthcoming*)
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd. Suite 1710
Los Angeles, California 90010
Tel: (213) 474-3800
Fax: (213) 471-4160
Email: daniel@slfla.com

A. Brooke Murphy (*pro hac vice forthcoming*)
MURPHY LAW FIRM
4116 Wills Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Tel: (405) 389-4989
Email: abm@murphylegalfirm.com

Gary M. Klinger (*pro hac vice forthcoming*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
Email: gklinger@milberg.com

Nicholas A. Migliaccio (*pro hac vice forthcoming*)
Jason S. Rathod (*pro hac vice forthcoming*)
MIGLIACCIO & RATHOD LLP
412 H St. NE, Suite 302
Washington, D.C. 20002
Tel: (202) 470-3520
Fax: (202) 800-2730
Email: nmigliaccio@classlawdc.com
Email: jrathod@classlawdc.com

Tyler J. Bean (*pro hac vice forthcoming*)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
Email: tbean@sirillp.com

Taylor Bartlett (BAR170)
HENINGER GARRISON DAVIS, LLC
2224 1st Avenue N.
Birmingham, AL 35203
Tel: (205) 326-3336
Email: taylor@hgdlawfirm.com

Annesley H. DeGaris (DEG002)
Alexandra J. Calton (CAL089)
DEGARIS LAW, LLC
2 North 20th Street, Suite 1030
Birmingham, AL 35203
Tel: (205) 575-8000
Fax: (205) 278-1454

Email: adegaris@degarislaw.com
Email: acalton@degarislaw.com

Counsel for Representative Plaintiffs and the Proposed Class