IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

BRET WOODALL, individually and on behalf of all others similarly situated, Plaintiff, v. OCTAPHARMA PLASMA, INC. Defendant.	Case No. 3:24-cv-00424-MOC-SCR **CLASS ACTION** JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Jean S. Martin
Morgan & Morgan Complex Litigation Group
201 N. Franklin St., 7th Floor
Tampa, FL 33602
813-559-4908
jeanmartin@forthepeople.com

Daniel Srourian
Srourian Law Firm, P.C.
3435 Wilshire Blvd.
Suite 1710
Los Angeles, CA 90010
213-474-3800
daniel@slfla.com

Beena M. McDonald
Chimicles Schwartz Kriner & Donaldson-Smith LLP
361 W. Lancaster Avenue
Haverford, PA 19041
610-642-8500
bmm@chimicles.com

Jeffrey M. Ostrow
Kopelowitz Ostrow Ferguson Weiselberg Gilbert
1 W. Las Olas Blvd., Suite 500
Ft. Lauderdale, FL 33301
954-525-4100
ostrow@kolawyers.com

Plaintiffs Kevin David Allport, Judy Kay Bishop, Karoline McKay, Labri Melzer, Timothy Taylor, and Jacob Borrero ("Plaintiffs"), individually, and on behalf of all others similarly situated as defined below (collectively, "Class Members"), by and through their undersigned counsel, allege the following against Octapharma Plasma, Inc. ("Defendant" or "Octapharma"). The following allegations are based upon Plaintiffs' personal knowledge as to themselves, and upon information and belief as to all other matters, including the investigation conducted by Plaintiffs' counsel.

INTRODUCTION

1. Plaintiffs seek to hold Defendant responsible for the injuries inflicted on Plaintiffs and Class Members arising from the targeted cyberattack and data breach that occurred on April 17, 2024, which was caused by Defendant's inadequately protected computer systems and information network, and which resulted in the unauthorized access to Plaintiffs' and Class Members' personally identifiable information ("PII")[1] and protected health information ("PHI")[2] (the "Data Breach").

2. Defendant "collects, tests and supplies human blood plasma" to develop and produce medicines.[3]

3. As a condition of receiving services, Defendant's plasma donors are required to provide and entrust Defendant with sensitive and private information, including PII and PHI (together "Private Information"), which Plaintiffs and Class Members provided to Defendant with the understanding that their sensitive and private information would be kept safe.

[1] PII generally includes information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information, such as names, dates of birth, addresses, email addresses, payment card information, and Social Security numbers.

[2] PHI refers to an individual's medical records and history, and may include, among other sensitive information, medical record numbers, health plan beneficiary numbers, treatment information, diagnosis information, test results and/or other medical information. PHI is protected by the Health Insurance Portability and Accountability Act ("HIPAA"), which requires certain healthcare entities such as Defendant to implement reasonable measures to protect PHI.

[3] https://www.octapharmausa.com/plasma/.

4. On April 17, 2024, Defendant detected unauthorized activity within its computer systems and/or network.[4] Defendant determined that an unauthorized third party breached its network and disrupted operations for the company.[5] The breach affected 176 of Defendant's donation centers in the United States, causing the centers to temporarily close from April 17 to April 22, 2024, while Defendant investigated the incident.[6]

5. On or about April 24, 2024, the ransomware group known as Black Suit claimed that it had breached and stolen sensitive Private Information from Defendant's network.[7] Black Suit claimed that the stolen information included patient names, Social Security numbers, dates of birth, addresses, laboratory data, financial data, employee data, business data, and other data taken from shared and personal folders.[8]

6. Since the announcement of the Data Breach, Defendant has offered no assurance to Plaintiffs and Class Members that the Private Information that was accessed in the Data Breach has been recovered or destroyed, or that it has adequately enhanced its security practices to avoid a breach of its network in the future.

7. By taking possession and control of Plaintiffs' and Class Members' Private Information, Defendant assumed a duty to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect its donors' Private Information from unauthorized disclosure.

8. Defendant also assumed duties to adequately safeguard its donors' sensitive and private information under a myriad of industry standards and federal and state statutes, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Section 5 of the

[4] https://www.octapharma.com/news/corporate-news/2024/news-update.
[5] *Id.*
[6] *Id.*; https://www.hipaajournal.com/octapharma-ransomware-attack/; https://therecord.media/plasma-donation-company-cyberattack-blacksuit.
[7] https://www.cyberdaily.au/security/10466-exclusive-black-suit-ransomware-gang-claims-hack-on-octapharma-plasma.
[8] *Id.*

Federal Trade Commission Act ("FTC Act"), and various state consumer protection statutes.

9. Instead of following these laws, however, Defendant breached its duties and disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. Defendant's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

10. Defendant breached its duties by, among other things, failing to sufficiently train its employees on cybersecurity and failing to implement and maintain reasonable security procedures and practices to protect its donors' Private Information from unauthorized access and disclosure. In short, Defendant's failures placed Plaintiffs' and Class Members' Private Information in a vulnerable position—rendering Plaintiffs and Class Members easy targets for cybercriminals.

11. The exposure of a person's Private Information through a data breach substantially increases that person's risk of identity theft, fraud, misappropriation of health insurance benefits, and other forms of criminal mischief, potentially for the rest of his or her life. The Private Information exposed in the Data Breach can enable criminals to commit a litany of crimes. Criminals can open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' health information to craft phishing and other hacking attacks based on Class Members' individual health needs, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest. Mitigation of such risk requires individuals to expend a significant amount of time and money to closely monitor their credit, financial accounts, health records, and email accounts. Mitigation of the risk of misuse of their sensitive Private Information may not even be

possible.

12. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiffs' and Class Members' Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

13. The Data Breach occurred as a direct and proximate result of Defendant's inadequate security and breach of its duties and obligations, because of which Plaintiffs' and Class Members' Private Information was accessed and disclosed. Plaintiffs and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of the benefit of their bargain; (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) anxiety, annoyance, and nuisance; (k) continued risk to their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information; and (l) disgorgement damages associated with Defendant's maintenance and use of Plaintiffs' and Class Members' data for its benefit and profit.

14. Through this action, Plaintiffs, on behalf of themselves and all other Class Members whose Private Information was exposed in the Data Breach, seek to remedy these injuries and assert claims for negligence, breach of fiduciary duty, breach of implied contract, breach of confidence, unjust enrichment, invasion of privacy, and violations of state law.

15. Plaintiffs seek remedies including, but not limited to, actual, nominal, and putative damages, appropriate injunctive and declaratory relief, and attorneys' fee, costs and expenses.

PARTIES

A. Plaintiffs

Plaintiff Kevin David Allport

16. Plaintiff Kevin David Allport is a natural person, resident, and citizen of Corvallis, Oregon.

17. Plaintiff Allport was a customer of Octapharma in approximately 2017-2018.

18. Plaintiff Allport received a notice of the Data Breach from Octapharma on or about August 30, 2024.

19. At the time of the Data Breach, Defendant retained Plaintiff Allport's Private Information in its computer network.

20. Plaintiff Allport was and is very careful about sharing his Private Information. Plaintiff Allport stores any documents containing Private Information in a safe and secure location. Plaintiff Allport would not have entrusted his Private Information with Defendant had he known of Defendant's failure to implement and maintain data security measures.

21. Upon information and belief, Plaintiff Allport's Private Information was unlawfully accessed and disclosed in the Data Breach.

22. Plaintiff Allport is not aware of ever being part of a data breach involving his Private Information and is concerned that it and other private information has now been exposed to bad actors. As a result, he has taken multiple steps to avoid identity theft, enrolling in increased credit monitoring, contacting attorneys, and researching the breach.

23. Plaintiff Allport has spent approximately one hour responding to the Data Breach.

24. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Private Information for theft by cybercriminals and sale on the dark web.

25. Plaintiff suffered actual injury from the exposure of his Private Information — which violates his rights to privacy.

26. Since the Data Brach, Plaintiff Allport has noticed an increase in the number of phishing emails he has received.

27. Plaintiff Allport has experienced increased fear over the possibility of being a victim of fraud since the Data Breach, which is amplified by the fact that key details about the Data Breach are still unknown, and Plaintiff Allport's Private Information is at continued risk of being stolen and used for fraudulent activity.

28. Plaintiff Allport greatly values his privacy and would not have provided his Private Information or used Defendant's services if he had known that his Private Information, including his Social Security number and health information, would be maintained using inadequate data security systems.

29. As a result of the Data Breach, Plaintiff Allport has suffered actual injury, is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Plaintiff Allport has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Judy Kay Bishop

30. Plaintiff Judy Kay Bishop is a natural person, resident, and citizen of Silvis, Illinois.

31. Plaintiff Bishop is a former plasma donor at Octapharma.

32. As a condition of donating plasma to Defendant, Plaintiff Bishop was required to provide her Private Information to Defendant, including her name, Social Security number, and full health and financial information.

33. At the time of the Data Breach, Defendant retained Plaintiff Bishop's Private Information in its system.

34. Plaintiff Bishop is very careful about sharing her sensitive Private Information. Plaintiff Bishop stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Bishop would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

35. Plaintiff Bishop received a notice regarding the Data Breach from Octapharma in September 2024.

36. At the time of the Data Breach, Defendant retained Plaintiff Bishop's Private Information in its system.

37. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Private Information for theft by cybercriminals and sale on the dark web.

38. Plaintiff suffered actual injury from the exposure of her Private Information — which violates her rights to privacy.

39. The Data Breach has caused Plaintiff Bishop to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about Data Breach.

40. As a result of the Data Breach, Plaintiff Bishop has spent considerable time researching the breach, monitoring her accounts for fraud, and contacting an attorney. Plaintiff Bishop estimates that she has spent a total of three to four hours attempting to respond to the Data Breach.

41. Since the Data Breach, Plaintiff Bishop has noticed a notable increase in the number of spam calls she has received.

42. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff's Private Information is here as a result of the Breach, cybercriminals are able to use the

stolen and compromised to gather and steal even more information.[9] On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

43. As a result of the Data Breach, Plaintiff Bishop has suffered actual injury, is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Plaintiff Bishop has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Jacob Borrero

44. Plaintiff Jacob Borrero is a natural person, resident, and citizen of Los Angeles, California.

45. Plaintiff Borrero formerly donated plasma with Defendant from approximately 2022 to 2024.

46. As a condition of donating Plasma to Defendant, Plaintiff Borrero was required to provide his Private Information to Defendant, including his name, Social Security number, phone number, email address, and full health and financial information.

47. At the time of the Data Breach, Defendant retained Plaintiff Borrero's Private Information in its system.

48. On or around August 30, 2024, Plaintiff Borrero received a letter from Defendant stating that his Private Information was involved in the Data Breach, including his name, health information, and donor eligibility information.

49. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Private Information for theft by cybercriminals and sale on the dark web.

50. Plaintiff suffered actual injury from the exposure of his Private Information — which violates his rights to privacy.

[9] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

51. After the Data Breach and as a result of the Data Breach, Plaintiff Borrero shas received an increase in spam calls, text messages and emails.

52. The increase in spam messages and emails also provides strong evidence that Plaintiff Borrero's Private Information was exfiltrated during the Data Breach and is now available or was available and sold on the Dark Web. These messages come from cyber criminals who gained access to the Private Information involved in the Data Breach due to exfiltration of the Private Information and dissemination on the Dark Web.

53. As a result of the Data Breach, Plaintiff Borrero has spent hours responding to the Data Breach, including researching the Data Breach, researching credit monitoring, reviewing his credit, and contacting attorneys. This time can never be recaptured.

54. Plaintiff Borrero is very careful about sharing his sensitive Private Information. Plaintiff Borrero 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. Plaintiff Borrero would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

55. The Data Breach has caused Plaintiff Borrero to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence. Plaintiff Borrero was so concerned that he ceased providing Plasma to Defendant after learning of the Data Breach.

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

57. As a result of the Data Breach, Plaintiff Borrero has suffered actual injury, is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Plaintiff Borrero has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and

safeguarded from future breaches.

58. On September 23, 2024, Plaintiff Borrero sent Octapharma Plasma, Inc. notice of Defendant's violations of and Plaintiffs' claims (and the claims of all others similarly situated) arising under the California Consumer Privacy Act ("CCPA") Section 1798.150 of the California Civil Code. To date, Defendant has failed to cure its violation of the CCPA and cannot cure its violation of the CCPA as Plaintiff Borrero's Private Information has already been disseminated to cybercriminals.

Plaintiff Karoline McKay

59. Plaintiff Karoline McKay is a natural person, resident, and citizen of Los Angeles, California.

60. Plaintiff McKay was a plasma donor of Defendant approximately from December 2022 through March 2023. She was required to submit her Private Information to Defendant as a condition of donating plasma, including her name, fingerprints, Social Security number, and full health and financial information.

61. At the time of the Data Breach, Defendant retained Plaintiff McKay's Private Information in its system.

62. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Private Information for theft by cybercriminals and sale on the dark web.

63. Plaintiff suffered actual injury from the exposure of her Private Information — which violates her rights to privacy.

64. Plaintiff McKay was and is very careful about sharing her Private Information. Plaintiff McKay stores any documents containing her Private Information in a safe and secure location. Plaintiff McKay would not have entrusted her Private Information to Defendant had she known of Defendant's failure to implement and maintain adequate data security measures.

65. Plaintiff McKay first learned of the Data Breach on or about September 30, 2024, as she was researching Octapharma for another reason.

66. Plaintiff McKay did not receive a breach notification letter from Defendant, however, upon calling Defendant for information about the Data Breach she was notified by Defendant that her information was on file and was likely compromised. Defendant offered credit monitoring to Plaintiff McKay.

67. Additionally, Plaintiff McKay learned from Defendant that Defendant had an old home address on file for her.

68. Upon information and belief, Plaintiff McKay's Private Information was unlawfully accessed and disclosed in the Data Breach.

69. Shortly after the Data Breach, in Spring 2024, Plaintiff McKay was notified by Bank of America of unauthorized charges on her credit accounts which amounted to approximately $500. Plaintiff disputed the charges and received a new credit card number.

70. About one month later, Plaintiff noticed additional unauthorized charges which amounted to approximately $500 on her new credit card. Plaintiff disputed the charges and received yet another credit card number.

71. Plaintiff McKay has also experienced an influx of phishing texts and calls since the Data Breach.

72. After the Data Breach, Plaintiff McKay was notified that her driver's license number was on the dark web.

73. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff's Private Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[10] On information and belief, Plaintiff's driver's license and phone number was compromised as a result of the Data Breach.

74. Since the Data Breach occurred, Plaintiff McKay has been required to spend valuable time communicating with her bank to combat the bank fraud alleged above and

[10] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

monitoring her various other accounts in an effort to detect and prevent any further misuse of her Private Information, time she would not have had to spend but for the Data Breach.

75. Plaintiff McKay estimates that she spent approximately three hours per day to address the bank fraud she experienced after the Data Breach. Her actions included communicating with her bank and the police about the fraud, monitoring her bank accounts, and closing other accounts in fear of future theft.

76. Plaintiff McKay estimates that she currently spends one to three hours per week to monitor her accounts by taking actions such as checking her bank statements and checking her credit report periodically on Experian.

77. Plaintiff McKay is now fearful of, and suffers paranoia and anxiety from, the ongoing risk of identity theft, fraud, and financial ruin since the Data Breach, which is amplified by the fact that key details about the Data Breach are still unknown, and Plaintiff McKay's Private Information is at continued risk of being stolen and used for fraudulent activity.

78. Plaintiff McKay greatly values her privacy and would not have provided her Private Information or become a donor if she had known that her Private Information, including her fingerprint, Social Security number, and health information, would be maintained using inadequate data security systems.

79. As a result of the Data Breach, Plaintiff McKay has suffered actual injury, is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Plaintiff McKay has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Labri Melzer

80. Plaintiff Labri Melzer is a natural person, resident, and citizen of California.

81. Plaintiff Melzer donated plasma with Defendant around March and April 2024.

82. As a condition of donating Plasma to Defendant, Plaintiff Melzer was required to

provide her Private Information to Defendant, including her name, Social Security number, phone number, email address, and full health and financial information.

83. At the time of the Data Breach, Defendant retained Plaintiff Melzer's Private Information in its system.

84. On or around August 30, 2024, Plaintiff received a letter from Defendant stating that her Private Information was involved in the Data Breach, including her name, health information, and donor eligibility information. The notice letter intentionally does not list in detail what of Plaintiff Melzer's information was subject to the Data Breach.

85. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Private Information for theft by cybercriminals and sale on the dark web.

86. Plaintiff suffered actual injury from the exposure of her Private Information — which violates her rights to privacy.

87. After the Data Breach and as a result of the Data Breach, Plaintiff Melzer has received an increase in spam calls, text messages and emails. Plaintiff Melzer started receiving text messages about job offers for remote jobs that do not exist. Many persons who donate plasma with Defendant do so to receive extra money at an easy and convenient location. These spam messages are easily related to the Data Breach as they prey on people who are likely to be interested in remote work or looking to make additional money. From the Data Breach, cyber criminals were able identify Plaintiff Melzer as a person who donates plasma and could likely be interested in remote work. Cybercriminals were then able to look up public information, including Plaintiff Melzer's phone number, to send her spam text messages that contain hazardous links to fraudulent and false remote work.

88. After the Data Breach, Plaintiff Melzer also began receiving text messages claiming to be UPS or FedEx. These messages contain a spam link and provide little context, attempt to get Plaintiff Melzer to click on the hazardous link. These text messages are phishing for additional information from Plaintiff Melzer and provide hazard links that contain malware.

89. As a result of the Data Breach, Plaintiff Melzer has received fraudulent and spam emails, including emails attempting to pose as PayPal informing her that large sums of money will be withdrawn from account if she does not take action.

90. The increase in spam messages and emails also provides strong evidence that Plaintiff Melzer's Private Information was exfiltrated during the Data Breach and is now available or was available and sold on the Dark Web. These messages come from cyber criminals who gained access to the Private Information involved in the Data Breach due to exfiltration of the Private Information and dissemination on the Dark Web.

91. As a result of the Data Breach, Plaintiff Melzer has spent hours responding to the Data Breach, including researching the Data Breach, researching credit monitoring, reviewing her credit reports, and reviewing her account statements. This time can never be recaptured.

92. Plaintiff Melzer is very careful about sharing her sensitive Private Information. Plaintiff Melzer stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Melzer would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

93. The Data Breach has caused Plaintiff Melzer to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence. Plaintiff Melzer has spent days worried that her medical information is readily available on the Dark Web.

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

95. As a result of the Data Breach, Plaintiff Melzer has suffered actual injury, is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Plaintiff Melzer has a continuing interest in ensuring that her Private Information, which, upon

information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

96. On September 12, 2024, Plaintiff Melzer sent Octapharma Plasma, Inc. notice of Defendant's violations of and Plaintiffs' claims (and the claims of all others similarly situated) arising under the California Consumer Privacy Act ("CCPA") Section 1798.150 of the California Civil Code. Defendant received Plaintiff Melzer's notice on September 19, 2024. To date, Defendant has failed to cure its violation of the CCPA and cannot cure its violation of the CCPA as Plaintiff Melzer's Private Information has already been disseminated to cybercriminals.

97. On September 12, 2024, Plaintiff Melzer sent Octapharma Plasma, Inc. a notice of demand under the California Consumer Legal Remedies Act ("CLRA") pursuant to under Cal. Civ. Code § 1782, notifying Defendant of its violations of the CLRA and Plaintiff Melzer's claims (and the claims of all others similarly situated) arising therefrom. Defendant received Plaintiff Melzer's notice on September 19, 2024. To date, Defendant has failed to cure its violation of the CLRA and cannot cure its violation of the CLRA as Plaintiff Melzer's Private Information has already been disseminated to cybercriminals.

Plaintiff Timothy Taylor

98. Plaintiff Timothy Taylor is a natural person, resident, and citizen of Los Angeles, California.

99. Plaintiff Taylor has been a plasma donor of Defendant since at least 2012 and was required to submit his Private Information to Defendant as a condition of donating plasma, including his name, Social Security number, and full health and financial information.

100. At the time of the Data Breach, Defendant retained Plaintiff Taylor's Private Information in its system.

101. Plaintiff Taylor was and is very careful about sharing his Private Information. Plaintiff Taylor stores any documents containing Private Information in a safe and secure location.

Plaintiff Taylor would not have entrusted his Private Information with Defendant had he known of Defendant's failure to implement and maintain data security measures.

102. Plaintiff Taylor first learned of the Data Breach after receiving notice from Octapharma in April 2024 that donation centers would be closed due to a security event.

103. Plaintiff Taylor then received a breach notification letter from Defendant on or about August 30, 2024, informing him that his Private Information was compromised in the Data Breach.

104. Upon information and belief, Plaintiff Taylor's Private Information was unlawfully accessed and disclosed in the Data Breach.

105. Plaintiff suffered actual injury from the exposure of his Private Information — which violates his rights to privacy.

106. Beginning shortly after the Data Breach, Plaintiff Taylor received an influx of phishing calls, text messages and emails.

107. Plaintiff Taylor has been receiving multiple spam messages each day, including phishing messages. For example, he received a text message from someone purporting to be the United States Postal Service and requesting confirmation of his personal information via an unsecured link.

108. The emails Plaintiff Taylor received and continues to receive are particularly worrisome. These emails attach fraudulent bills seeking payments amounting to hundreds of dollars.

109. Additionally, one email received by Plaintiff Taylor on September 15, 2024, threatened to release sensitive information about him to the public unless he paid $1300.

110. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff's Private Information is here as a result of the Breach, cybercriminals are able to use the

stolen and compromised to gather and steal even more information.[11] On information and belief, Plaintiff's email address and phone number was compromised as a result of the Data Breach.

111. On or about September 30, 2024, Plaintiff Taylor received notification from the Employment Development Department that the pin number to his benefits account was changed. Plaintiff Taylor did not authorize this change. Plaintiff Taylor has been in contact with Employment Development Department to investigate and redress the attempted fraud.

112. Since the Data Breach occurred, Plaintiff Taylor has been required to spend valuable time monitoring his various accounts to detect and prevent any misuse of his Private Information, time he would not have had to spend but for the Data Breach.

113. Plaintiff Taylor estimates that he spends roughly 10-12 hours per week since the Data Breach to monitor his accounts by taking actions such as blocking calls, text messages, and emails from unknown sources and checking his credit report weekly on Experian. Plaintiff Taylor additionally monitors Defendant's website for updates.

114. Plaintiff Taylor is now fearful of, and suffers paranoia and anxiety from, the ongoing risk of identity theft, fraud, and financial ruin since the Data Breach, which is amplified by the fact that key details about the Data Breach are still unknown, and Plaintiff Taylor's Private Information is at continued risk of being stolen and used for fraudulent activity.

115. Plaintiff Taylor greatly values his privacy and would not have provided his Private Information or become a donor if he had known that his Private Information, including his Social Security number and health information, would be maintained using inadequate data security systems.

[11] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

116. As a result of the Data Breach, Plaintiff Taylor has suffered actual injury, is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Plaintiff Taylor has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

B. Defendant

117. Defendant Octapharma Plasma, Inc., is a Delaware corporation with its principal place of business located at 10644 Westlake Drive in Charlotte, North Carolina 28273. Upon information and belief, Defendant is the U.S. subsidiary of Octapharma AG, a global healthcare company headquartered in Lachen, Switzerland, with more than 195 donation centers around the world and with hundreds of thousands of patients in 118 countries.[12]

118. Defendant is engaged in the industry of collecting lifesaving plasma from donors throughout the United States and across the world and is "one of the largest human protein product manufacturers in the world."[13]

JURISDICTION AND VENUE

119. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative members, in which some members of the class are citizens of states different than Defendant, and the amount in controversy exceeds $5,000,000 dollars, exclusive of interest and costs.

120. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

121. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District, and regularly conducts business in this District, and has sufficient minimum contacts in this District.

[12] https://www.octapharmaplasma.com/our-vision/; https://www.octapharma.com/api/download/x/df5a28c67e/annual-report-2023_english.pdf.
[13] https://www.octapharma.com/about-us/who-we-are.

122. Venue is proper under 28 U.S.C. § 1391 because Defendant's headquarters is in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Defendant Collects and Stores the Private Information of Plaintiffs and Class Members

123. Defendant is the United States subsidiary of Octapharma AG, a pharmaceutical entity that "collects, tests and supplies human blood plasma" to develop and produce medicines based on the collection of human plasma.[14] It is the largest privately owned plasma fractionator in the world with locations in 118 countries.[15]

124. Defendant operates more than 195 plasma collection sites and employs over 11,000 individuals throughout Europe and the United States.[16] Upon information and belief, most of Defendant's plasma donation centers are in the United States.[17]

125. As a condition of collecting plasma from donors, Defendant requires that its donors entrust it with sensitive and private information such as their names, dates of birth, addresses, Social Security numbers, and financial information in the ordinary course of its business. Defendant also collects sensitive personal information, including health and medical information, medical history, insurance information, billing information, medical records, photo identification, and more. Upon information and belief, Defendant collects and maintains the aforementioned Private Information on its network.

126. In the course of their relationship with Defendant, as donors of Defendant, Plaintiffs and Class Members provided Defendant with their Private Information. In doing so, Plaintiffs and Class Members relied on Defendant to keep their sensitive Private Information confidential and secured, to use such information for healthcare and business purposes only, and

[14] https://www.octapharmausa.com/plasma/.
[15] https://www.octapharmausa.com/about-us.
[16] https://www.octapharmausa.com/about-us/who-we-are.
[17] https://www.octapharmaplasma.com/plasma-donation-centers/.

to make only authorized disclosures of this information.

127. Due to its status as a healthcare entity, and due to the highly sensitive nature of the Private Information Defendant collects and maintains, Defendant knew or should have known of its obligations to provide confidentiality and adequate security for donor safety under federal and state law, health industry standards, or otherwise through its own applicable policies, including its Privacy Policy.

128. Indeed, Defendant both explicitly and implicitly promised Plaintiffs and Class members that it used reasonable measures to safeguard the Private Information it collects from theft and misuse.

129. Recognizing its legal and equitable duties, Defendant represented in its Privacy Statement that:

> Octapharma Plasma, Inc. … respects the right of individuals regarding the disclosure and use of their personal information.
> ***
> We collect information from and about users of our website, unregistered and registered (individually "User" and collectively, "Users") including information by which you may be personally identified, such as your name, e-mail address, physical address, telephone number, as well as a variety of other personal information such as information about your demographic profile and interests ("Personal Information"). The information we collect on or through our website may include information that you provide to us by registering to use our website, using our website or our services, entering information into a form or other data entry fields available on our website, posting materials, requesting further services or reporting a problem with our website. We will also retain records and copies of your correspondence (including email addresses) if you contact us.
> ***
> To maintain data accuracy and ensure the correct use of information, we have put in place procedures to safeguard and secure the information we collect online."[18]

130. Additionally, Defendant's Privacy Statement states that it only discloses Private Information to third parties in certain circumstances, none of which involve the circumstances of the Data Breach.[19]

[18] https://www.octapharmaplasma.com/privacy-legal/.
[19] *Id.*

131. Defendant misrepresented to Plaintiffs and Class Members via its Privacy Statement that it has procedures in place to safeguard Private Information. Upon information and belief, including from information gathered from the Data Breach at issue, that representation is not true.

132. Had Plaintiffs and Class Members known that Defendant did not have the measures in place to keep their sensitive and private information confidential and secure, they would not have provided such information to Defendant.

133. Unfortunately, Defendant's failure to adequately protect its computer systems and network as described throughout this Consolidated Class Action Complaint resulted in the Data Breach and caused actual injuries to Plaintiffs and Class members.

The Data Breach

134. On or about April 17, 2024, Defendant "detected suspicious activity on its network."[20] In response, it launched an investigation into the source of the disruption and took all systems offline, which involved closing all plasma donation centers located in the United States.[21] Defendant was clear that its plasma donation centers in Germany and Europe were not impacted in the security event.[22]

135. Notably, Defendant has yet to disclose the specific details of the attack. Defendant has made only three brief statements regarding the Data Breach, none of which explain the specifics about the attack, including when the breach occurred or the full spectrum of information stolen.[23]

136. The lack of information that has come from Defendant since the Data Breach is evidence that it is deliberately underplaying the significance of the Data Breach, and intends to place the burden on the victims, many of which had no idea that the breach occurred until they

[20] https://www.octapharma.com/news/corporate-news/2024/news-update.
[21] *Id.*
[22] *Id.*
[23] *Id.*

learned about it from the news.

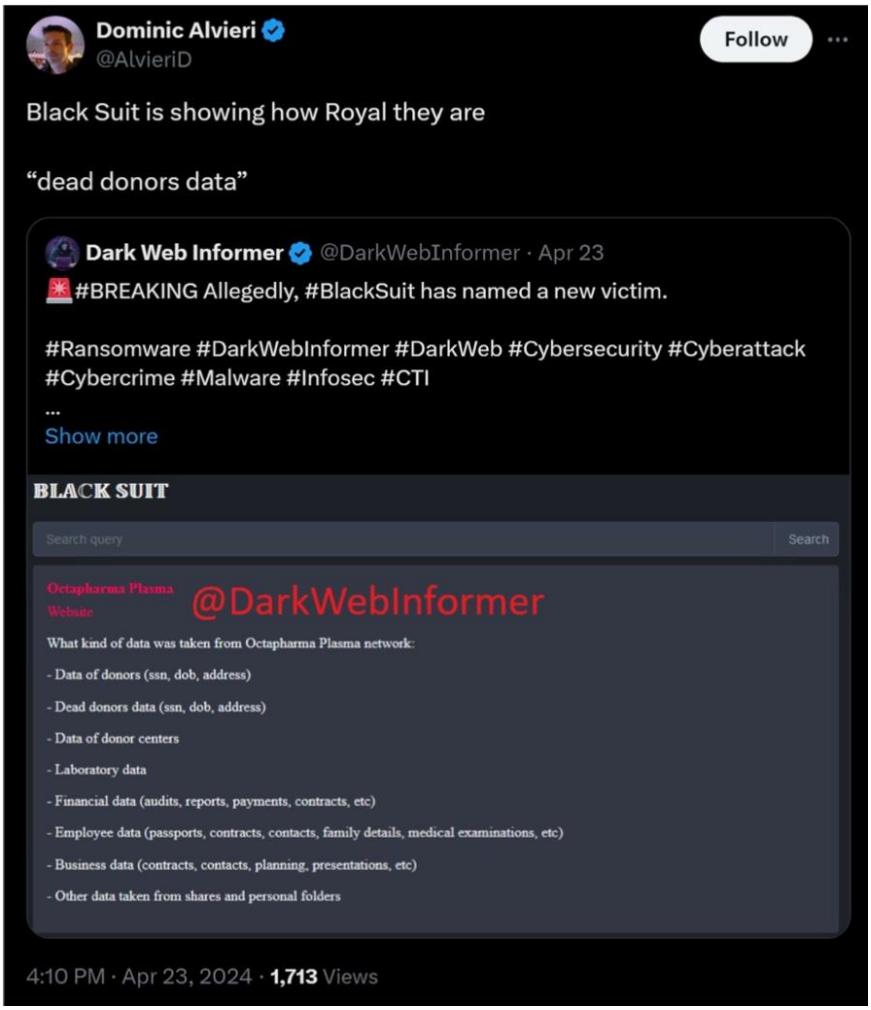
137. The bulk of the reporting on the specifics of the event have come from the bad actor, the ransomware group Black Suit, itself.

138. On or about April 24, 2024, the ransomware group Black Suit took responsibility for the attack, claiming that it had not only accessed, but also exfiltrated, extremely sensitive Private Information from Defendant during the Data Breach.[24] Black Suit claimed that the stolen information includes "patient names, Social Security numbers, dates of birth, addresses, laboratory data, financial data, employee data, business data, and other data taken from shares and personal folders."[25]

[24] David Hollingworth, *Exclusive: BlackSuit Ransomware Gang Claim Hack on Octapharma Plasma*, cyberdaily.au, https://www.cyberdaily.au/security/10466-exclusive-black-suit-ransomware-gang-claims-hack-on-octapharma-plasma.
[25] *Id*.

139. With the Private Information secured and stolen, the hackers then purportedly issued a ransom demand to Defendant. However, Defendant has provided no public information on the ransom demand or payment.

140. On information or belief, Black Suit released all stolen information onto the dark web for access, sale, and download following the deadline of the ransom demand to Defendant.



141. A ransomware attack is a type of cyberattack that is frequently used to target entities due to the sensitive data they maintain.[26] In a ransomware attack the attackers use

[26] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/

software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[27]

142. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[28] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

143. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[29] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[30] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[31] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[32]

144. Upon information and belief, at the time of the Data Breach, Plaintiffs' and Class Members' Private Information was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

---

[27] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs
[28] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends
[29] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/
[30] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report
[31] *Id*.
[32] *Id*.

145. Upon information and belief, the cyberattack was targeted at Defendant due to its status as a healthcare entity that collects, creates, and maintains Private Information on its computer network and/or systems. Defendant knew or should have known that cybercriminals like Black Suit would target it.

146. Healthcare entities, such as Defendant, were notified by the U.S. Department of Health and Human Services ("HHS") in November 2023 that the sector is at risk for an attack from Black Suit.[33]

147. Based on the unfortunate events described throughout this Consolidated Class Action Complaint, Defendant did not heed HHS's warning and failed to take action to prevent the Data Breach by implementing adequate data security measures to protect its computer systems and network from unauthorized breach, resulting in the compromise and acquisition of Plaintiffs' and Class Members' Private Information in the Data Breach.

148. Defendant chose to keep Plaintiffs and Class Members in the dark about the Data Breach, providing them as little information as possible and failing to immediately issue breach notification letters, thereby placing the burden on Plaintiffs and Class Members to take measures to protect themselves from identity theft and fraud because of the Data Breach.

149. Cybercriminals frequently publish stolen Private Information to the dark web and make it available for purchase. As the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[34]

150. Plaintiffs believe that their Private Information was, or soon will be, published to

[33] American Hospital Association, *HHS alerts health care sector to new ransomware threat* (Nov. 9, 2023), https://www.aha.org/news/headline/2023-11-09-hhs-alerts-health-care-sector-new-ransomware-threat.

[34] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

the dark web and made available to purchase.

151. Plaintiffs and Class Members now face a present, heightened, and continued threat of identity theft and other types of criminal mischief resulting from the Data Breach, potentially for the rest of their lives, all of which was completely preventable by Defendant.

Private Information is Valuable and Defendant Knew the Risks Associated with Storing that Private Information

152. At all relevant times, Defendant knew, or should have known, that Plaintiffs' and Class Members' Private Information was a target for cybercriminals. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyberattacks.

153. Defendant also knew that any breach of its computer systems and networks, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

154. By acquiring, collecting, and using Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties created by the HIPAA, the FTC Act, industry standards, contract law, common law, and statutory law to keep Plaintiffs' and Class Members' Private Information confidential, and to protect it from unauthorized access and disclosure.

155. Defendant's data security obligations were of particular importance due to the steady increase over the years of data breaches targeting medical information.

156. The healthcare industry is a known target for cybercriminals. "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[35] Healthcare entities are also more likely to pay a hacker's

[35] Swivel Secure, *The healthcare industry is at risk*, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/.

ransom due to the sensitive information that such entities maintain and collect, and because they have an incentive to regain access to their data quickly.[36]

157. The number of data breaches experienced by healthcare entities continues to rise. In a 2024 report, the healthcare compliance company Protenus found that there were 942 medical data breaches in 2023, leaving over 171 million patient records exposed. This is an increase from the 905 medical data breaches that Protenus compiled in 2021.[37]

158. According to Mimecast, a cybersecurity firm, 90% of healthcare organizations experienced cyberattacks in 2020.[38]

159. The last several years have been marked by several high-profile healthcare data breaches including, but not limited to:

- Emergency Medical Services Authority (611,743 patients, March 2024);
- Risas Dental & Braces (618,189 patients, March 2024);
- Eastern Radiologists, Inc., (886,746 patients, February 2024);
- Ann & Robert H. Lurie Children's Hospital (791,784 patients, January 2024);
- MCNA Dental (8,900,000 patients, March 2023);
- Broward Health (1,300,000 patients, January 2022);
- Morley (521,046 patients, February 2022);
- Regal Medical Group (3,300,000 patients, December 2022);
- Trinity Health (3,300,000 patients, March 2020);
- Shields Healthcare Group (2,000,000 patients, March 2022); and
- One Touch Point (2,600,000 individuals, July 2022).

[36] Elise Takahama, *Why health care has become a top target for cybercriminals*, The Seattle Times https://www.seattletimes.com/seattle-news/health/why-health-care-has-become-a-top-target-for-cybercriminals/.
[37] *2024 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report.
[38] Maria Hernandez, *Iowa City Hospital Suffers Phishing Attack*, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

160. An article from April 23, 2024, discussed the latest findings in Baker Hostetler's tenth annual Data Security Incident Response Report, which found that despite companies' adeptness at responding to cyberattacks from criminals, "ransomware attacks show no signs of abating."[39] Moreover, "[c]ombating these attacks has also been complicated by hackers' practice of constantly innovating and evolving their methods in order to get around the controls and safeguards that businesses are erecting to counter their attacks."[40]

161. Defendant certainly knew and understood that unprotected or exposed Private Information in the custody of healthcare entities, like Defendant, is valuable and highly sought after by criminals seeking to illegally monetize that Private Information through unauthorized access.

162. Defendant also knew or should have known that Private Information is a valuable property right, leading to the purchase of said data by American companies. American companies spent over $19 billion on acquiring personal data of consumers in 2018.[41] The buying and selling of consumer data comprises the data broker industry, which is believed to be worth over $200 billion dollars.[42]

163. One way that criminals profit from stolen Private Information is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen Private Information, and second, unregulated data found elsewhere on the internet (like phone numbers, email addresses, physical addresses, etc.).

---

[39] Allison Grande, *Ransomware Still on the Rise Despite Better Defenses, Firm Says*, LAW 360 (Apr. 23, 2024), https://www.law360.com/articles/1827647/ransomware-still-on-rise-despite-better-defenses-firm-says.

[40] *Id.*

[41] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[42] David Lazarus, *Shady data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES, Nov. 5, 2019, https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

164. The development of "Fullz" packages means that the Private Information exposed in the Data Breach can easily be linked to data of Plaintiffs and Class Members that is already available on the internet. In other words, even if certain information such as email addresses, phone numbers, or credit card numbers may not have been included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) repeatedly. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

165. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's online credentials or Social Security number. "Social engineering" is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these targeted attacks.

166. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[43] Criminals favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[44] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

167. A sophisticated black market exists on the dark web where criminals can buy or

[43] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/
[44] *Id.*

sell malware, firearms, drugs, and, frequently, personal and medical information like the Private Information at issue in this case.[45] The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and both buyer and seller can retain anonymity, unlike the sale of a firearm or drugs, which requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[46] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[47]

168. Private Information is a valuable commodity on the black market.[48] Numerous sources cite dark web pricing for stolen identity credentials.[49]

169. For example, Private Information can be sold at a price ranging from $40 to $200.[50] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[51]

170. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[52] In 2021, it was reported that stolen healthcare records can fetch for as much as $1000

[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.
[49] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/
[50] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/
[51] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/
[52] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

on the black market.[53] That price is likely much higher today.

171. The Federal Bureau of Investigation's ("FBI") Cyber Division reports that criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[54]

172. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[55]

173. Consumers also place a high value on the privacy of their data. Studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[56] Recently, more consumers are exercising their Data Subject Access Rights and leaving providers over their data practices and policies.[57]

174. Companies like Defendant are no doubt aware of the value that is placed on sensitive Private Information and that cybercriminals continue to successfully target that data to obtain significant profits. As such, companies like Defendant must remain on high alert and must

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

[54] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[55] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

[56] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), available for download at: https://www.jstor.org/stable/23015560?seq=1.

[57] CISCO, *Cisco 2023 Consumer Privacy Survey* (April 2023), available at https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html?CCID=cc000742.

act in accordance with their legal and equitable obligations, and industry standards, to implement reasonable security measures to prevent targeted data attacks aimed at their patients' Private Information.

175. Considering the value of Private Information, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

176. Defendant breached its duties by failing to implement and maintain reasonable security measures to protect Plaintiffs' and Class Members' Private Information from being stolen which caused the Data Breach and resulted in harm to Plaintiffs and Class Members, who now face imminent and continuing risk of identity theft and fraud.

177. Defendant exposed the Private Information of Plaintiffs and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information. Defendant's failure to promptly and properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injuries by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

The Theft of Private Information Has Grave and Lasting Consequences for Plaintiffs and Class Members

178. The theft of Private Information is costly for those affected. A cybercriminal who steals a person's Private Information can end up with as many as "seven to 10 personal identifying characteristics of an individual."[58]

[58] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon

179. According to Experian, one of the largest credit reporting agencies:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[59]

180. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank or financial fraud. They can obtain and use personal data to open a new credit card or take out a loan, open a bank account and write bad checks, apply for government benefits, take over existing debit and credit accounts, withdraw funds, and even obtain medical procedures.[60]

181. The FTC also warns consumers about various types of identity theft.[61] Criminals

---

[59] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/#:~:text=Gather%20Documents%20and%20File%20Reports,call%20800%2DHHS%2DTIPS.

[60] Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[61] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft.

can obtain a driver's license or official identification card in the victim's name, but with the thief's picture, and then use the victim's name and Social Security Number to obtain government benefits or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number; rent a house or receive medical services in the victim's name and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued for the victim.[62]

182. Alarmingly, a thief can use stolen medical information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[63]

183. Identity theft is not an easy problem to solve. The Identity Theft Resource Center found that most victims of identity crimes need more than a week to resolve issues stemming from identity theft and some need months to a year.[64]

184. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[65]

185. Here, not only was sensitive medical information compromised, but Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities

[62] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.
[63] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon
[64] Identity Theft Resource Center, 2023 Consumer Impact Report, available for download at: https://www.idtheftcenter.org/publications/.
[65] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

186. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [66] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[67]

187. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[68] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[69]

188. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[70]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

---

[66] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.
[67] *Id.*
[68] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/
[69] *See* https://www.investopedia.com/terms/s/ssn.asp
[70] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), https://www.gao.gov/assets/270/262904.html.

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

189. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

190. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as in the instant case, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[71]

191. Moreover, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraudulent activity to obtain a new Social Security number.

192. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[72]

---

[71] Social Security Administration, Identity Theft and Your Social Security Number, https://www.ssa.gov/pubs/EN-05-10064.pdf

[72] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

193. Victims of medical identity theft face another set of problems. A report published by the World Privacy Forum and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected;
- Significant bills for medical goods and services not sought nor received;
- Issues with insurance, co-pays, and insurance caps;
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft;
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime;
- Denial of mortgages and other financial impacts as a result of improper and/or fraudulent medical debt reporting;
- Phantom medical debt collection based on medical billing or other identity information; and
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[73]

194. Further complicating victims' ability to defend themselves from identity theft is the time lag between when Private Information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to

[73] World Privacy Forum, *The Geography of Medical Identity Theft* (Dec. 12, 2017), available for download at: https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.

learn that information.[74] Criminals may deliberately wait years before they decided to use stolen data.

195. A healthcare entity that deals with the sensitive Private Information of its patients is legally required to safeguard such information from unauthorized access and disclosure to third parties due to inherent sensitivity of the Private Information and the grave and long-lasting consequences that can result from any unauthorized access and disclosure.

196. Defendant has failed to comply with its legal obligations to protect its donors', including Plaintiffs' and Class Members', Private Information, which caused the Data Breach. As a result of the Data Breach, Plaintiffs and Class Members now live with their Private Information exposed in cyberspace and available to people willing to purchase and use the information for any number of improper purposes and crimes.

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

Defendant Breached its Legal Duties to Protect Private Information

A. Defendant Violated HIPAA

198. The Health Insurance Portability and Accountability Act ("HIPAA") requires covered entities to implement reasonable security measures to protect patient information, including protected health information (PHI), defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

199. HIPAA further prohibits the unauthorized disclosure of protected health information and circumscribes security provisions and data privacy responsibilities designed to

[74] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

keep patients' medical information safe.

200. Defendant is a HIPAA-covered entity that provides healthcare services. *See* 45 C.F.R. § 160.12. As a regular and necessary part of its business, Defendant collects and maintains Private Information of patients.

201. HIPAA requires Defendant to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information by adopting the requirements set forth in HIPAA's Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information), and HIPAA's Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information"). These rules are commonly known as the Administrative Simplification Rules and establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.

202. Defendant is also required to report any unauthorized use or disclosure of such protected information, including incidents of a data breach "without unreasonable delay and in no case later than 60 days following discovery of the breach."[75] *See* 45 C.F.R. § 164.404(b).

203. As an entity covered by HIPAA, Defendant assumed legal obligations and knew or should have known that it was responsible for safeguarding Plaintiffs' and Class Members sensitive and private information from unauthorized disclosure.

204. As set forth throughout this Consolidated Class Action Complaint, Defendant did not implement the required safeguards it is required to maintain under HIPAA. Defendant did so with knowledge of its legal duties under HIPAA and of the risks associated with unauthorized access to Plaintiffs' and Class Members' PHI.

205. Defendant's HIPAA violations include but are not limited to the following:

a. Failing to notify affected individuals without unreasonable delay and in no

[75] Breach Notification Rule, U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

case later than 60 days following discovery of the breach. 45 C.F.R. §164.404(b);

b. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits. 45 C.F.R. § 164.306(a)(1);

c. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of PHI. 45 C.F.R. § 164.306(a)(2);

d. Failing to protect against any reasonably anticipated uses or disclosure of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information. 45 C.F.R. § 164.306(a)(3);

e. Failing to ensure compliance with HIPAA security standards by Defendant's workforce. 45 C.F.R. § 164.306(a)(4);

f. Failing to review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information. 45 C.F.R. § 164.306(e);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights. 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain and correct security violations. 45 C.F.R. § 164.308(a)(1);

i. Failing to identify and respond to suspected or known security incidents and failing to mitigate the harmful effects of security incidents that are known. 45 C.F.R. § 164.308(a)(6)(ii);

j. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI. 45 C.F.R. § 164.530(b); 45 C.F.R. § 164.308(a)(5); and

k. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI. 45 C.F.R. § 164.530(c).

206. As a result of Defendant's failure to comply with HIPAA regulations, cybercriminals circumvented Defendant's lax security measures, resulting in the Data Breach and

injuring Plaintiffs and Class Members.

B. Defendant Violated the FTC Act

207. Additionally, the Federal Trade Commission Act ("FTC Act") prohibits Defendant from engaging in "unfair or deceptive acts or practices in or affecting commerce." *See* 15 U.S.C. § 45.

208. According to the FTC, the need for data security should be factored into all business decision-making. To that end, the FTC has promulgated numerous guides for what data security principles and practices businesses must use to protect against the exposure of Private Information.[76]

209. The FTC's publication, *Protecting Personal Information*, established cyber-security guidelines for businesses. The guidelines declare that businesses must:

l. take action to protect the personal patient information that they collect;

m. properly dispose of personal information that is no longer needed;

n. encrypt information stored on computer networks;

o. understand their networks' vulnerabilities; and

p. implement policies to correct any security problems.[77]

210. The guidelines also recommend that businesses:

q. use an intrusion detection system to expose a breach as soon as it occurs;

r. monitor all incoming traffic for activity indicating someone is attempting to hack the system;

s. watch for large amounts of data being transmitted from the system; and

t. have a response plan ready in the event of a breach.[78]

[76] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

[77] *Id.*

[78] *Id.*

211. The FTC further recommends that businesses:

u. not maintain private information longer than is needed for authorization of a transaction;

v. limit access to sensitive information;

w. require complex passwords be used on networks;

x. use industry-tested methods for security monitor for suspicious activity on the networks; and

y. verify that third-party service providers have implemented reasonable security measures.

212. Section 5 of the FTC Act, 15 U.S.C. § 45 gives the FTC the authority to bring enforcement actions against businesses for failing to adequately and reasonably protect Private Information. . Thus, the FTC treats the failure to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTC Act. The orders that result from enforcement actions further clarify the measures businesses must take to meet their data security obligations.

213. Defendant failed to properly implement basic data security practices despite being aware at all relevant times of its obligations to protect Plaintiffs' and Class Members' Private Information, and of the significant consequences that would result from its failure to do so.

214. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

215. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. Industry standards for healthcare providers such as Defendant exist because of the high threat of cyberattacks that target the sensitive information that healthcare entities collect and maintain.

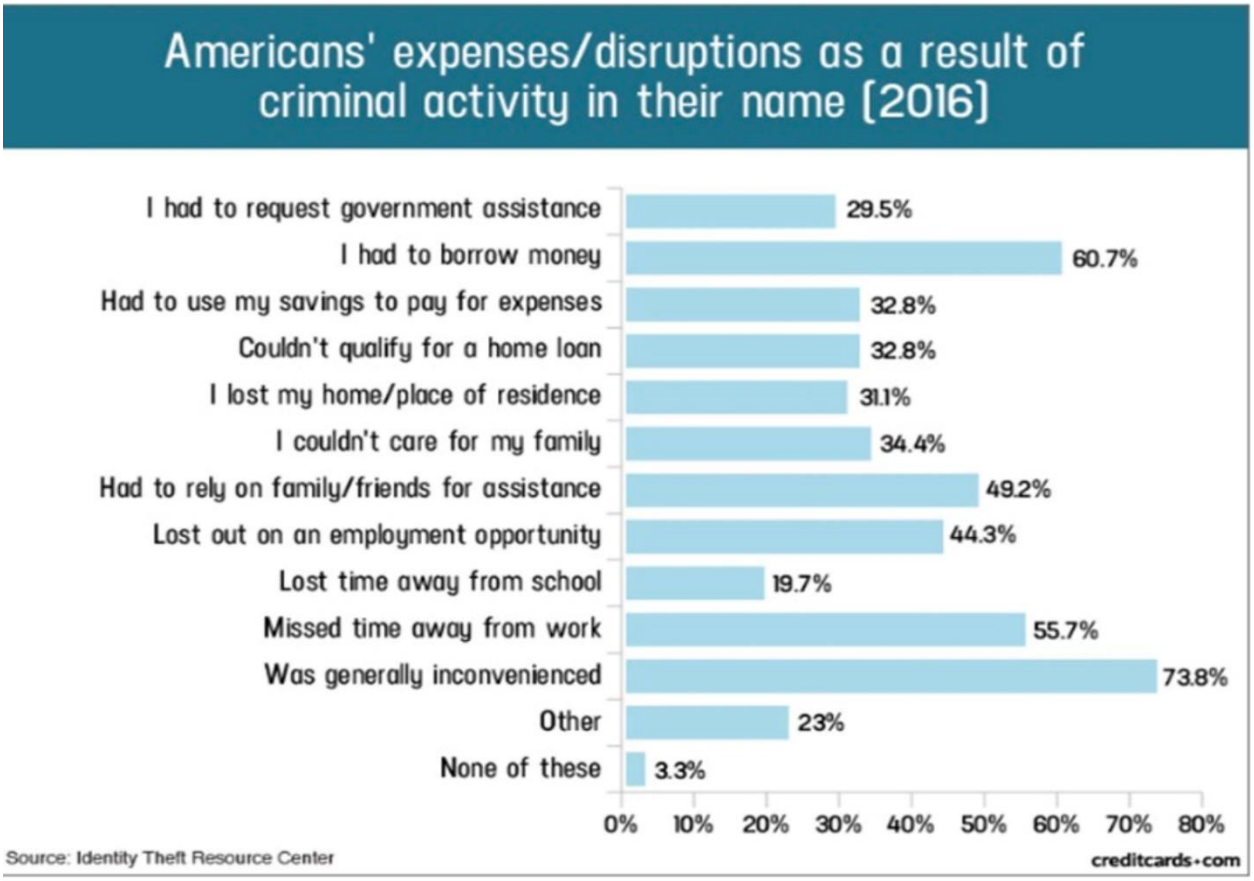
216. These best practices include, but are not limited to: educating and training employees about the risks of cyberattacks; requiring the use of strong passwords; implementing multi-layer security such as firewalls; installing anti-virus and malware software; encrypting data; using multi-factor authentication; backing up data; limiting the number of employees with access to sensitive data; setting up network firewalls, switches and routers; monitoring and limiting network ports; and monitoring and limiting access to physical security systems.

217. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

218. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach and the resulting harm to Plaintiffs and Class Members.

Plaintiffs and Class Members Sustained Common Damages as a Result of the Data Breach

219. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:



220. Once Private Information 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, Plaintiffs and Class Members will need to maintain the heightened measures mentioned below for years, and possibly for their entire lives, as a result of Defendant's conduct.

Plaintiffs and Class Members are at an Imminent and Continuing Risk of Future Fraud and Identity Theft

221. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members

has materialized and is imminent. Plaintiffs and Class Members have suffered injury and will continue to suffer damages including monetary losses, lost time, anxiety, and emotional distress. Plaintiffs and Class Members have suffered or are at increased risk of suffering:

a. fraudulent bank accounts, loans, and/or utility bills opened in their name;

b. medical services billed in their names;

c. out of pocket expenditures for protective and remedial services;

d. improper disclosure of their Private Information;

e. breach of the confidentiality of their Private Information;

f. invasion of their privacy;

g. deprivation of the value of their Private Information, for which there is a well-established national and international market;

h. the loss of the benefit of the bargain; and/or

i. lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the continued and increased risks of identity theft and medical identity theft.

222. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

Plaintiffs and Class Members Lost Time Mitigating the Risk of Identity Theft and Fraud

223. Plaintiffs and Class Members must immediately devote time, energy, and money to:

a. closely monitoring their Social Security numbers, medical statements, bills, records, and credit and financial accounts for unauthorized activity for years to come;

b. contacting financial institutions and closing or modifying financial

accounts;

c. reviewing and monitoring financial and other sensitive accounts for fraudulent insurance claims, loans, and/or government benefits claims;

d. placing credit freezes and alerts with reporting agencies;

e. changing login and password information on any sensitive account even more frequently than they already do;

f. more carefully screening and scrutinizing phone calls, texts, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and

g. searching for suitable identity theft protection and credit monitoring services, and paying to procure them.

Plaintiffs and Class Members Suffered a Diminution in Value of Their Private Information

224. In 2019, the data brokering industry was worth roughly $200 billion.[79]

225. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[80]

226. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $60.00 a year.[81]

227. Conversely, as mentioned above, Private Information can be sold on the dark web at prices ranging from $40 to $200, depending on the type of information sold.[82] According to the Infosec Institute, sensitive Private Information can sell for as much as $363 per record on the dark

[79] David Lazarus, *Shady data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES, Nov. 5, 2019, https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[80] *See., e.g.*, https://datacoup.com/
[81] Nielsen Computer & Mobile Panel, Frequently Asked Questions, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html
[82] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

web.[83]

228. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

The Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

229. Given the type of targeted attack in this case and sophisticated criminal activity involved in the Data Breach – including the admission of the ransomware group known as Black Suit taking responsibility for the Data Breach, claiming that they stole sensitive Private Information from Defendant's network – there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes–e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

230. Moreover, because some of this information, like names and Social Security Numbers, is immutable, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

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

232. The retail cost of credit monitoring and identity theft monitoring can cost around $200 per year per Class Member. This is a reasonable and necessary cost to monitor to protect

[83] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://www.infosecinstitute.com/resources/healthcare-information-security/hackers-selling-healthcare-data-in-the-black-market/

Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost that Plaintiffs and Class Members will need to bear for a minimum of five years, and which they would not need to bear but for Defendant's failure to safeguard their Private Information.

Plaintiffs and Class Members Lost the Benefit of Their Bargain

233. Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to provide their Private Information, which was a condition precedent to being a paid donor or obtaining services, and getting paid or paying Defendant for its services, Plaintiffs, as consumers, understood and expected that they were, in part, being paid less in order to pay for data security to protect the Private Information required to be collected from her.

234. However, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what was reasonably expected to receive or was paid less than bargained for under the bargains struck with Defendant.

CLASS ALLEGATIONS

235. Plaintiffs bring this class action pursuant to Federal Rule of Civil Procedure 23(a). 23(b)(2), and 23(b)(3) individually and on behalf of all members. Plaintiffs intend to seek certification of the Nationwide Class or, in the alternative, the California, Oregon, and/or Illinois Subclasses (collectively, "State Subclasses") set forth below.

236. The **Nationwide Class** that Plaintiffs seek to represent is defined as:

> All individuals in the United States whose Private Information was compromised in the Data Breach that was announced April 17, 2024 (the "Nationwide Class" or "Class").

237. The **California Subclass** that Plaintiff Borrero, Plaintiff McKay, Plaintiff Melzer, and Plaintiff Taylor seek to represent:

> All individuals in state of California whose Private Information was compromised in the Data Breach that was announced April 17, 2024 (the "California Subclass").

238. The **Oregon Subclass** that Plaintiff Allport seeks to represent:

> All individuals in state of Oregon whose Private Information was compromised in the Data Breach that was announced April 17, 2024 (the "Oregon Subclass").

239. The **Illinois Subclass** that Plaintiff Bishop seeks to represent:

> All individuals in state of Illinois whose Private Information was compromised in the Data Breach that was announced April 17, 2024 (the "Illinois Subclass").

240. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

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

242. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

243. **Numerosity.** The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. While the exact number of individuals affected is unknown, Defendant reported that the Data Breach has affected 190 plasma donation centers across 35 states, potentially affecting thousands of individuals. The contact information

of those individuals is available from Defendant's business records.

244. **Commonality.** Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' Private Information;

c. Whether Defendant a breached its duties to protect Plaintiffs' and Class Members' Private Information;

d. Whether Defendant breached its fiduciary duty to Plaintiffs and Class Members;

e. When Defendant learned of the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring procedures were deficient;

g. Whether hackers obtained Plaintiffs' and Class Members' data in the Data Breach;

h. Whether an implied contract existed between Plaintiffs and Class Members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure;

i. Whether Defendant was unjustly enriched;

j. Whether Defendant's conduct violated various states' consumer protection and privacy statutes;

k. Whether Plaintiffs and Class Members are entitled to injunctive relief and

identity theft protection to redress the imminent harm they face due to the Data Breach; and

l. Whether Plaintiffs and Class Members are entitled to damages and the measure of such damages and relief.

245. **Typicality.** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their Private Information compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

246. **Adequacy of Representation.** Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

247. **Superiority.** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class Members to individually seek redress from Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

248. All proposed Class Members are readily ascertainable. Defendant has access to

the names, addresses, and/or email addresses of Class Members affected by the Data Breach.

249. Finally, class certification is appropriate under FED. R. CIV. P. 23(b). Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of himself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

CAUSES OF ACTION

250. Plaintiffs bring these causes of action on behalf of the Nationwide Class and State Subclasses as defined herein. The application of one specific state's laws to any cause of action is premature at this juncture, without the benefit of discovery, as Defendant maintains servers and plasma donation centers in several states, and plasma donors of Defendant's exist in several states across the country.

COUNT I
VIOLATION OF NORTH CAROLINA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT
(N.C. Stat. § 75-1.1, *et. seq.*)
(On Behalf of Plaintiffs and the Nationwide Class)

251. Plaintiffs, individually and on behalf of the Nationwide Class, incorporate by reference paragraphs 1 through 234 as if fully set forth herein.

252. The North Carolina Unfair and Deceptive Trade Practices Act ("NCUDTPA" or the "Act") prohibits "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" N.C. Gen. Stat. § 75- 1.1(a).

253. Under the Act, "commerce" includes "all business activities, however, denominated[.]" *Id.* at § 75-1.1(b).

254. Furthermore, "any person . . . injured . . . by reason of any act or thing done by any other person, firm or corporation in violation of this Chapter, such person . . . so injured shall have a right of action on account of such injury done[.]" *Id.* at § 75-16.

255. Defendant's conduct was unfair and deceptive in violation of the Act. Specifically,

Defendant represented that they could adequately protect Plaintiffs' and Class Members' Private Information and that its platforms were safe and secure. It obtained donors through these representations and, in turn, gained access to and control over Plaintiffs' and Class Members' Private Information.

256. Defendant, however, could not adequately protect Plaintiffs' and Class Members' Private Information, and designed an insecure platform lacking reasonable data security measures that were entirely inadequate to protect the highly sensitive data it collected and stored.

257. Under N.C. Gen. Stat. §§ 75-61, 75-65, businesses impacted by a data breach must provide notice without reasonable delay. Defendant, however, failed to adequately notify Plaintiffs and Class Members of the scope and extent of the Data Breach.

258. Defendant's conduct was, thus, unethical, unscrupulous, substantially injurious to Plaintiffs and Class Members, and against North Carolina's stated policy of quickly providing notice of a data breach.

259. Defendant engaged in the conduct alleged in this Consolidated Class Action Complaint through transactions in and involving trade and commerce.

260. As alleged herein this Consolidated Class Action Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement adequate data security practices to safeguard its current and former donors' Private Information;

b. failure to make only authorized disclosures of its current and former donors' Private Information;

c. failure to disclose that their data security practices were inadequate to safeguard Private Information from theft; and

d. failure to timely and accurately disclose the Data Breach to Plaintiffs and Class Members.

261. Defendant's actions constitute unconscionable, deceptive, or unfair acts or

practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Defendant's current and former donors who are Plaintiffs and Class Members.

262. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing Plaintiffs' and Class Members' Private Information, and that they did not follow industry best practices for the collection, use, and storage of Private Information.

263. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been harmed and have suffered actual damages in an amount to be proven at trial, 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; (vii) experiencing an increase in spam calls, texts, and/or emails; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

264. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiffs and Class Members have been damaged and are entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

265. Also, as a direct result of Defendant's knowing violation of the North Carolina Unfair and Deceptive Trade Practices Act, Plaintiff and Class Members are entitled to injunctive relief, including, but not limited to ordering that Defendant: (i) implement measures that ensure

that the Private Information of Defendant's current and former donors is appropriately encrypted and safeguarded when stored on Defendant's network or systems; (ii) purge, delete, and destroy in a reasonable secure manner Private Information it does not need to keep; (iii) routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (iii) meaningfully educate its donors about the threats they face as a result of the accessibility of their Private Information to third parties, as well as the steps Defendant's donors must take to protect themselves.

COUNT II
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

266. Plaintiffs reallege and incorporate by reference paragraphs 1 through 234 as if fully set forth herein.

267. Defendant requires that its donors, including Plaintiffs and Class Members, submit Private Information in the course of providing its medical services.

268. Defendant collected, acquired, and stored Plaintiffs' and Class Members' Private Information.

269. Plaintiffs and Class Members entrusted Defendant with their Private Information and had the understanding that Defendant would safeguard their information.

270. Defendant had knowledge of the sensitivity of Plaintiffs' and Class Members' Private Information, and the consequences that would result from the unauthorized disclosure of such information. Defendant knew that healthcare entities were the target of cyberattacks in the past, and that Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate data security procedures.

271. It was therefore reasonably foreseeable that the failure to implement adequate data security procedures would result in injuries to the Plaintiffs and Class Members.

272. Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable

care in safeguarding and protecting their Private Information in its possession, custody, or control from the unauthorized disclosure of such information.

273. Defendant's duty to exercise reasonable care arises from several sources, including but not limited to common law, the HIPPA, the FTCA, and industry standards.

274. Defendant's duty also arose from its position as a healthcare provider. As a healthcare provider, Defendant assumed a duty to exercise reasonable care in safeguarding and protecting donors' private information in its possession, custody, or control from the unauthorized disclosure of such information.

275. Defendant's duties also arose from, inter alia, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

276. Defendant's duties also arose from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant of failing to employ reasonable measures to protect and secure Private Information.

277. Defendant violated HIPAA Privacy and Security Rules, Section 5 of the FTCA, UCL, CMIA, and CCPA by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtains and stores, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

278. Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence *per se*.

279. Plaintiffs and Class Members are within the class of persons that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

280. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

281. Defendant breached its duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Private Information entrusted to it—including Plaintiffs' and Class Members' Private Information.

282. Defendant admitted that the Private Information of Plaintiffs and Class Members was disclosed to unauthorized third persons as a result of the Data Breach.

283. Defendant's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class Members caused their Private Information to be compromised in the Data Breach.

284. Plaintiffs and Class Members were in no position to protect their Private Information themselves.

285. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class Members' Private Information to unauthorized individuals.

286. But for Defendant's breach of the duties described herein, Plaintiffs and Class Members' Private Information would not have been compromised.

287. There is a causal relationship between Defendant's failure to implement, control,

direct, oversee, manage, monitor, and audit adequate data security procedures to protect the Private Information its donors and the harm suffered by Plaintiffs and Class Members.

288. As a direct and proximate result of Defendant's conduct described above, it directly and proximately caused the Data Breach, and Plaintiffs and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

289. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

290. Plaintiffs and Class Members are entitled to damages incurred as a result of the Data Breach.

291. Defendant's negligent conduct is ongoing, in that it still holds Plaintiffs' and Class Members' Private Information in an unsafe and insecure manner.

292. Plaintiffs and Class Members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Plaintiffs and Class Members.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class)

293. Plaintiffs reallege and incorporate by reference paragraphs 1 through 234 as if fully set forth herein.

294. Plaintiffs and Class Members gave Defendant their Private Information in confidence, believing that Defendant would protect that information. Plaintiffs and Class Members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiffs' and Class Members' Private Information created a fiduciary relationship between Defendant and Plaintiffs and Class Members. In light of this relationship, Defendant must act primarily for the benefit of its donors, which includes safeguarding and protecting Plaintiffs' and Class Members' Private Information.

295. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship – especially to secure their Private Information.

296. Because of the highly sensitive nature of their Private Information, Plaintiffs and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

297. Defendant breached their fiduciary duty by failing to properly protect the computer systems and network containing Plaintiffs' and Class Members' Private Information; failing to comply with the data security guidelines set forth by HIPAA and the FTCA; and failing to sufficiently encrypt or otherwise safeguard Plaintiffs' and Class Members' Private Information that it collected.

298. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of

Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

299. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

300. Plaintiffs and Class Members are entitled to damages incurred as a result of the Data Breach.

301. Plaintiffs and Class Members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

302. Plaintiffs reallege and incorporate by reference paragraphs 1 through 234 as if fully set forth herein.

303. In connection with donating plasma or other medical services, Plaintiffs and Class Members entered into implied contracts with Defendant or were intended third-party beneficiaries of contracts between Defendant and others.

304. Pursuant to these implied contracts, plasma was provided to Defendant by

Plaintiffs and Class Members, and Defendant was provided with Private Information of Plaintiffs and Class Members. In exchange, Defendant implicitly agreed to, among other things, take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' Private Information and protect Plaintiffs' and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

305. The protection of Private Information was a material term of the implied contracts that were either between Plaintiffs and Class Members, on the one hand, and Defendant, on the other hand, or were between third parties and Defendant to which Plaintiffs and Class Members were intended third-party beneficiaries.

306. Plaintiffs and Class Members, or the third parties, fulfilled their obligations under the contracts.

307. Defendant breached its obligations by failing to implement and maintain reasonable data security measures to protect and secure the Private Information and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class Members' Private Information in a manner that complies with applicable laws, regulations, and industry standards.

308. Defendant's breach of its obligations of its implied contracts directly resulted in the Data Breach and the injuries that Plaintiffs and Class Members have suffered from the Data Breach.

309. Plaintiffs and Class Members were damaged by Defendant's breach of implied contracts because: (i) they were promised data security they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) they suffered actual identity theft; (iv) their Private Information was improperly disclosed to unauthorized individuals; (v) the confidentiality of their Private Information has been breached; (vi) they were deprived of the value of their Private Information for which there is a well-established national

and international market; and/or (vii) they lost time and money to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

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

310. Plaintiffs reallege and incorporate by reference paragraphs 1 through 234 as if fully set forth herein.

311. This count is pleaded in the alternative to Plaintiffs' breach of implied contract claim (Count IV).

312. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of plasma paid to Defendant and/or its agents for healthcare services or other services.

313. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security procedures.

314. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members by acquiring and/or collecting their Private Information as a necessary part of obtaining Defendant's services. Defendant appreciated and benefitted from the receipt of Plaintiffs' and Class Members' Private Information and payments in that Defendant used the Private Information and profited from the healthcare transactions in furtherance of its business.

315. Defendant acquired Plaintiffs' and Class Members' Private Information and payments through inequitable means in that it failed to disclose the inadequate data security procedures previously alleged herein.

316. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between the payments they received from Defendant and the additional value that Defendant appropriated for itself by not protecting

Plaintiffs' and Class Members' Private Information with adequate security measures.

317. Defendant should not be permitted to retain the Private Information belonging to Plaintiffs and Class Members because Defendant failed to adequately implement the data privacy and security procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

318. Defendant unjustly enriched itself by using the plasma and Private Information acquired from Plaintiffs and Class Members to further its business.

319. Notably, Defendant chose not to use its profits to enhance its data security procedures.

320. Under principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiffs and Class Members and should be compelled to provide for the benefit of Plaintiffs and Class Members, all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VI
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Nationwide Class)

321. Plaintiffs reallege and incorporate by reference paragraphs 1 through 234 as if fully set forth herein.

322. During Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential nature of the Private Information that Plaintiffs and Class Members provided to it.

323. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by promises and expectations that Plaintiffs and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

324. Plaintiffs and Class Members provided their respective Private Information to

Defendant with the explicit and implicit understanding that Defendant would protect their Private Information and not permit their Private Information to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

325. Plaintiffs and Class Members also provided their Private Information to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect their Private Information from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting networks and data systems.

326. Due to Defendant's failure to prevent, detect and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices to secure Plaintiffs' and Class Members' Private Information, Plaintiffs' and Class Members' Private Information was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiffs' and Class Members' confidence and without their express permission.

327. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages, as alleged herein.

328. But for Defendant's failure to maintain and protect Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. The Data Breach was the direct and legal cause of the misuse of Plaintiffs' and Class Members' Private Information and the resulting damages.

329. The injury and harm Plaintiffs and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Plaintiffs' and Class Members' Private Information. Defendant knew its data systems and protocols for

accepting and securing Plaintiffs' and Class Members' Private Information had security and other vulnerabilities that placed Plaintiffs' and Class Members' Private Information in jeopardy.

330. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer injury, as alleged herein, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their Private Information, (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their Private Information, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Class Members' Private Information in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, (vii) the diminished value of Plaintiffs' and Class Members' Private Information, and (viii) the diminished value of Defendant's services.

COUNT VII
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class)

331. Plaintiffs incorporate by reference paragraphs 1 through 234 as if fully set forth herein.

332. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

333. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

334. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' Private Information would be highly offensive to a reasonable person.

335. The intrusion was into a place or thing which was private and entitled to be private.

336. Plaintiffs and Class Members disclosed their sensitive and confidential Private Information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

337. The Data Breach constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

338. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

339. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and Class Members in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

340. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

341. As a proximate result of Defendant's acts and omissions, the sensitive Private Information of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class Members to suffer damages (as detailed supra).

342. And, on information and belief, Plaintiffs' and other Class Members' Private Information has already been published—or will be published imminently—by cybercriminals on the dark web.

343. Unless and until enjoined and restrained by order of this Court, Defendant's

wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members since their Private Information is still maintained by Defendant with their inadequate cybersecurity system and policies.

344. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiffs and Class Members.

345. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class Members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT VIII
DECLARATORY JUDGMENT/INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Nationwide Class)

346. Plaintiffs incorporate by reference paragraphs 1 through 234 as if fully set forth herein.

347. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Consolidated Class Action Complaint

348. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Private Information and whether Defendant is currently maintaining adequate data security measures to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Plaintiffs allege that Defendant's data security measures remain inadequate, contrary to Defendant's assertion that the security of its network is no longer at risk. Plaintiffs continue to suffer injuries as a result of the compromise of

their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

349. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure Private Information and to timely notify donors or any individuals impacted of a data breach under the common law, Section 5 of the FTC Act, HIPAA, various state statutes, and common law; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure donors' Private Information.

350. This Court should also issue corresponding prospective injunctive relief requiring Defendant to, at minimum:

a. disclose, expeditiously, the full nature of the Data Breach and the types of Private Information accessed, obtained, or exposed by the hackers;

b. implement improved data security practices to reasonably guard against future breaches of Plaintiffs' and Class Members' Private Information possessed by Defendant;

c. provide, at its own expense, all impacted victims with lifetime identity theft protection services such as credit monitoring and identity theft insurance;

d. cease engaging in the wrongful and unlawful acts alleged herein;

e. delete and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

f. engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

g. conduct regular database scanning and securing checks; monitor ingress and egress of all network traffic;

h. establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

i. implement a system of tests to assess its respective employees' knowledge

of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

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

k. educate the public about the threats that it faces because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

351. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injuries, and lack adequate legal remedies, in the event of another data breach of Defendant's systems. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct

352. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

353. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach of Defendant's systems, thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose confidential information would be further compromised.

COUNT IX
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT
(Cal. Civ. Code §§ 1798.80, *et seq*.)
(On Behalf of Plaintiffs Borrero, McKay, Melzer and Taylor and the California Subclass)

354. Plaintiffs Borrero, McKay, Melzer, and Taylor ("Plaintiffs" for the purposes of

this Count), individually and on behalf of the California Subclass, incorporate by reference paragraphs 1 through 234 as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding customer records.

355. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires any "business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

356. Defendant is a business that owns, maintains, and licenses "personal information", within the meaning of Cal. Civ. Code § 1798.81.5(d)(1), which includes, *inter alia*, "medical information" and "health information," about Plaintiff and California Subclass members.

357. Businesses that own or license computerized data that includes personal information, including Social Security Numbers, medical information and health information, are required to notify California residents when their personal information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82. *Id.*

358. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82(h).

359. Plaintiffs' and California Subclass Members' Private Information includes "personal information" as covered by Cal. Civ. Code §§ 1798.81.5(d)(1), 1798.82(h).

360. Because Defendant reasonably believed that Plaintiffs' and California Subclass Members' Private Information was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

361. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Cal. Civ. Code § 1798.82.

362. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass Members suffered damages, as described above.

363. Plaintiffs and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT X
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW
(Cal. Civ. Code §§ 17200, *et seq*.)
(On Behalf of Plaintiffs Borrero McKay, Melzer, and Taylor and the California Subclass)

364. Plaintiffs Borrero, McKay, Melzer, and Taylor ("Plaintiffs" for the purposes of this Count), individually and on behalf of the California Subclass, incorporate by reference paragraphs 1 through 234 as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding customer records.

365. Defendant is a "person" as defined by Cal. Bus. & Prof. Code §17201.

366. Defendant violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

367. Defendant's unfair and deceptive acts and practices include:

a. Defendant's failure to implement and maintain reasonable security measures to protect Plaintiffs' and California Subclass members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

b. Defendant's failure to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents.

c. Defendant's failure to implement and maintain reasonable security measures also was contrary to public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws including California's Consumer Legal Remedies Act ("CLRA"), Cal Civ. Code § 1750, et seq. the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, et seq., HIPAA, the Confidentiality of Medical Information Act ("CMIA"), Cal Civ. Code § 56.36(b), and the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.82, et. seq.

d. Defendant's failure to implement and maintain reasonable security measures led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused.

e. Defendant's engagement in unlawful business practices by violating Cal. Civ. Code § 1798.82.

368. Defendant has engaged in unlawful business practices by violating multiple laws, including the CCPA, Cal. Civ. Code §§ 1798.80, et seq., the CLRA, Cal. Civ. Code §§ 1750, et seq., the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, et seq., HIPAA; and the CMIA, Cal. Civ. Code § 56.36(b).

369. Defendant's unlawful practices include:

a. Failure to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

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

c. Failure to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1750, et seq., the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, et seq., HIPAA, and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the Data Breach;

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

e. Misrepresentation that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass Members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1750, et seq., the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, et seq., HIPAA, and the CMIA, Cal. Civ. Code § 56.36(b);

f. Failure to timely and adequately notify the Plaintiff and California Subclass Members of the Data Breach;

g. Misrepresentation and/or omission of the fact that that certain sensitive Private Information was not accessed during the Data Breach, when it was;

h. Omission, suppression, and concealment of , the material fact that Defendant did not reasonably or adequately secure Plaintiff's and California Subclass Members' Private Information; and

i. Omission, suppression, and concealment of the material fact that Defendant did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1750, et seq., the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, HIPAA, and the CMIA, Cal. Civ. Code § 56.36(b). Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

370. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the California Subclass Members, into believing that their Private Information was not exposed and misled Plaintiffs and the California Subclass Members into believing they did not need to take actions to secure their identities.

371. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass Members were injured and lost money or property, including monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information, including but not limited to the diminishment of their present and future property interest in their Private Information and the

deprivation of the exclusive use of their Private Information.

372. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and California Subclass Members' rights.

373. Plaintiffs and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT XI
VIOLATION OF CALIFORNIA CONSUMER LEGAL REMEDIES ACT
(Cal. Civ. Code §§ 1750, *et seq*.)
(On Behalf of Plaintiffs Borrero, McKay, Melzer, and Taylor and the California Subclass)

374. Plaintiffs Borrero, McKay, Melzer, and Taylor ("Plaintiffs" for the purposes of this Count), individually and on behalf of the California Subclass, incorporate by reference paragraphs 1 through 219 as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding customer records.

375. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

376. Defendant is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770. Specifically, Defendant provides monetary compensation to customers that donate their plasma, which involves storing and managing Private Information of consumers.

377. As part of the services Defendant offers, Defendant both explicitly and implicitly promised Plaintiffs and California Subclass members that it used reasonable measures to safeguard the Private Information it collects from theft and misuse. Indeed, in its Privacy Statement Defendant touted that it "respects the right of individuals regarding the disclosure and use of their personal information" and that "[t]o maintain data accuracy and ensure the correct use of information, we have put in place procedures to safeguard and secure the information we collect online."[84]

378. Additionally, Defendant's Privacy Statement states that it only discloses Private Information to third parties in certain circumstances, none of which involve the circumstances of the Data Breach.[85]

379. Plaintiffs and the California Subclass are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

380. Defendant's acts and practices were intended to and did result in the sales of products and services to Plaintiffs and the California Subclass Members in violation of Civil Code § 1770, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, HIPAA, and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of

[84] *See* https://www.octapharmaplasma.com/privacy-legal/.
[85] *Id.*

Plaintiffs' and California Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, HIPAA, and the CMIA, Cal. Civ. Code § 56.36(b);

f. Failing to timely and adequately notify Plaintiffs and California Subclass Members of the Data Breach;

g. Misrepresenting that certain sensitive Private Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass Members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, HIPAA, and the CMIA, Cal. Civ. Code § 56.36(b).

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

382. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the California Subclass Members, into believing that their Private Information was not exposed and misled Plaintiffs and California Subclass Members into believing they did not need to take actions to secure their identities.

383. Had Defendant disclosed to Plaintiffs and California Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant was trusted with sensitive and valuable Private Information of consumers, including that of Plaintiffs and California Subclass Members.

384. Defendant accepted the responsibility of being a steward of this data while keeping

the inadequate state of its security controls secret from the public. Accordingly, because Defendant held itself out as maintaining a secure platform for Private Information data, Plaintiffs, and California Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

385. As a direct and proximate result of Defendant's violations of California Civil Code § 1770, Plaintiffs and California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, including but not limited to the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

386. On September 12, 2024, Plaintiff Melzer sent Octapharma Plasma, Inc. a notice of demand pursuant to under Cal. Civ. Code § 1782, notifying Defendant of its violations of the CLRA and Plaintiff Melzer's claims (and the claims of all others similarly situated) arising therefrom. Defendant received Plaintiff Melzer's notice on September 19, 2024. To date, Defendant has failed to cure its violation of the CLRA and cannot cure its violation of the CLRA as California Subclass Members' Private Information has already been disseminated to cybercriminals.

387. Plaintiffs and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

COUNT XII
VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT
(Cal. Civ. Code §§ 1798.100, *et seq*.)
(On Behalf of Plaintiffs Borrero, McKay, Melzer, and Taylor and the California Subclass)

388. Plaintiffs Borrero, McKay, Melzer, and Taylor ("Plaintiffs" for the purposes of

this Count), individually and on behalf of the California Subclass, incorporate by reference paragraphs 1 through 234 as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding customer records.

389. Plaintiffs and California Subclass Members are covered "consumers" under section 1798.140(g) in that they are natural persons who are residents of California.

390. Defendant is a "business" under section 1798.140(b) in that it is a corporation that is organized or operated for the profit or financial benefit of its shareholders or other owners, with annual global sales of €3.266 billion.[86]

391. Defendant is a business that collects, tests and supplies human blood plasma and with that collects consumers' personal information as defined by Cal. Civ. Code § 1798.140. Specifically, Defendant obtains, receives, and/or accesses consumers' personal information to use for business purposes when, *inter alia*, customers donate plasma to Defendant.

392. The Private Information of Plaintiffs and the California Subclass members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and § 1798.81.5, in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance

[86] https://www.octapharma.com/api/download/x/df5a28c67e/annual-report-2023_english.pdf

information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

393. Defendant determines the purposes and means of processing consumers' personal information. Defendant uses consumers' personal data to provide services to customers.

394. Defendant violated Section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiffs' and California Subclass Members' nonencrypted and nonredacted personal information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

395. Defendant knew or should have known that its data security practices were inadequate to secure Plaintiffs' and California Subclass Members' Private Information and that its inadequate data security practices gave rise to the risk of a data breach.

396. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the Private Information it collected and stored. The cybercriminals accessed "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(d)(1)(A), in the Data Breach.

397. Upon information and belief, Plaintiffs' and California Subclass Members' Private Information accessed by the cybercriminals in the Data Breach includes "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(d)(1)(A).

398. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.150, Plaintiffs and California Subclass Members suffered damages, as described above.

399. On September 12, 2024, Plaintiff Melzer sent Octapharma Plasma, Inc., notice of Defendant's violations of and Plaintiffs' claims (and the claims of all others similarly situated) arising under the California Consumer Privacy Act ("CCPA") Section 1798.150 of the California Civil Code. Defendant received Plaintiff Melzer's notice on September 19, 2024. To date,

Defendant has failed to cure its violation of the CCPA and cannot cure its violation of the CCPA as California Subclass Members' Private Information has already been disseminated to cybercriminals.

400. On September 23, 2024, Plaintiff Borrero sent Octapharma Plasma, Inc., notice of Defendant's violations of and Plaintiffs' claims (and the claims of all others similarly situated) arising under the California Consumer Privacy Act ("CCPA") Section 1798.150 of the California. To date, Defendant has failed to cure its violation of the CCPA and cannot cure its violation of the CCPA as California Subclass Members' Private Information has already been disseminated to cybercriminals.

401. Plaintiffs and California Subclass Members seek injunctive relief in the form of an order requiring Defendant to employ adequate security practices consistent with law and industry standards to protect Plaintiffs' and California Subclass Members' Private Information, requiring Defendant to complete its investigation, and to issue a statement giving a detailed explanation that confirms, with reasonable certainty, what categories of data were stolen and accessed without Plaintiffs' and California Subclass Members' authorization, along with an explanation of how the data breach occurred.

402. Plaintiffs and California Subclass Members seek statutory damages or actual damages, whichever is greater, pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

COUNT XIII
VIOLATION OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT
(Cal. Civ. Code § 56, *et seq*.)
(On Behalf of Plaintiffs Borrero, McKay, Melzer, and Taylor and the California Subclass)

403. Plaintiffs Borrero, McKay, Melzer, and Taylor ("Plaintiffs" for the purposes of this Count), individually and on behalf of the California Subclass, incorporate by reference paragraphs 1 through 234 as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding customer records.

404. Under the CMIA, California Civil Code §56.05(k), Plaintiffs and California Subclass Members (except employees of Defendant whose records may have been accessed) are deemed "patients."

405. As defined in the CMIA, California Civil Code §56.05(j), Defendant disclosed "medical information" to unauthorized persons without obtaining consent, in violation of §56.10(a). Defendant's misconduct, including failure to adequately detect, protect, and prevent unauthorized disclosure, directly resulted in the unauthorized disclosure of Plaintiffs' and California Subclass Members' Private Information to unauthorized persons. This information was subsequently viewed by unauthorized third parties as a direct result of this disclosure.

406. Defendant's misconduct, including protecting and preserving the confidential integrity of Defendants' clients'/customers' Private Information, resulted in unauthorized disclosure of sensitive and confidential Private Information that belongs to Plaintiffs and California Subclass Members to unauthorized persons, breaching the confidentiality of that information, thereby violating California Civil Code §§ 56.06 and 56.101(a).

407. Plaintiffs and California Subclass Members have all been and continue to be harmed as a direct, foreseeable, and proximate result of Defendants' breach because Plaintiffs and California Subclass Members face, now and in the future, an imminent threat of identity theft, fraud, and for ransom demands. They must now spend time, effort and money to constantly monitor their accounts and credit to surveille for any fraudulent activity.

408. Plaintiffs and California Subclass Members were injured and have suffered damages, as described above, from Defendant's illegal disclosure and negligent release of their Private Information in violation of Cal. Civ. Code §§ 56.10 and 56.101 and, therefore, seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

COUNT XIV
VIOLATION OF THE OREGON CONSUMER IDENTITY THEFT PROTECTION ACT
Or. Rev. Stat. §§ 646A.604(1), et seq.
(On Behalf of Plaintiff Allport and the Oregon Subclass)

409. Plaintiff Allport, individually and on behalf of the Oregon Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 219 above and incorporates the same as if set forth herein.

410. Octapharma is a "covered entity" that maintains records which contain personal information (for the purpose of this count, "Private Information"), within the meaning of § 646A.602(5) and Or. Rev. Stat. § 646A.622(1), about Plaintiff Allport and Oregon Subclass Members.

411. Pursuant to Or. Rev. Stat. § 646A.622(1), a "covered entity and a vendor shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information[.]"

412. Octapharma violated Or. Rev. Stat. § 646A.622(1) by failing to implement reasonable measures to protect Plaintiff's and Oregon Subclass Members' Private Information.

413. Octapharma is a "covered entity" that owns, maintains, or otherwise possesses data that includes consumers Private Information as defined by Or. Rev. Stat. § 646A.604(1).

414. Plaintiff's and Oregon Subclass Members' Private Information includes PII as covered under Or. Rev. Stat. § 646A.604(1).

415. Octapharma is required to accurately notify Plaintiff and Oregon Subclass Members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Or. Rev. Stat. § 646A.604(1).

416. Because Octapharma discovered a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Or. Rev. Stat. §§ 646A.604(1) and (3).

417. By failing to disclose the Data Breach in a timely and accurate manner, Octapharma violated Or. Rev. Stat. § 646A.604(1).

418. Pursuant to Or. Rev. Stat. § 646A.604(11), violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1) are unlawful practices under Or. Rev. Stat. § 646.607.

419. As a direct and proximate result of Octapharma's violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1), Plaintiff and Oregon Subclass Members suffered damages, as described above.

420. Plaintiff Allport and Oregon Subclass Members seek relief under Or. Rev. Stat. § 646.638, including actual damages, punitive damages, and injunctive relief.

COUNT XV
VIOLATION OF THE OREGON UNLAWFUL TRADE PRACTICES ACT
Or. Rev. Stat. §§ 646.605, et seq.
(On Behalf of Plaintiff Allport and the Oregon Subclass)

362. As a direct and proximate result of Octapharma's violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1), Plaintiff and Oregon Subclass Members suffered damages, as described above.

363. Plaintiff Allport, individually and on behalf of the Oregon Subclass, repeats and realleges the factual allegations set forth in paragraphs 1 through 219 above and incorporates the same as if set forth herein.

364. Octapharma is a "person," as defined by Or. Rev. Stat. § 646.605(4).

365. Octapharma engaged in the sale of "goods and services," as defined by Or. Rev. Stat. § 646.605(6)(a).

366. Octapharma sold "goods or services," as defined by Or. Rev. Stat. § 646.605(6)(a).

367. Octapharma advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

368. Octapharma engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, included the following:

a. Representing that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Advertising its goods or services with intent not to provide them as advertised;

d. Concurrent with tender or delivery of its goods and services, failing to disclose any known material defect.

369. Octapharma's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Information Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq*., which was a direct and proximate cause of the Data Breach;

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

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Information Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.;*

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

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed

by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Information Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq*.

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

371. Octapharma intended to mislead Plaintiff and Oregon Subclass Members and induce them to rely on its misrepresentations and omissions.

372. Had Octapharma disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Octapharma would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Octapharma was trusted with sensitive and valuable Private Information regarding consumers, including Plaintiff and Subclass Members. Octapharma accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public.

373. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Octapharma's misrepresentations and omissions, the truth of which they could not have discovered. Octapharma acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff and Oregon Subclass Members' rights. Octapharma's status in the healthcare industry put it on notice that healthcare entities were targets for data breaches.

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

375. Plaintiff and Oregon Subclass Members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages or statutory damages of $200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

COUNT XVI
VIOLATION OF THE ILLINOIS PERSONAL INFORMATION PROTECTION ACT
(815 Ill. Comp. Stat §§ 530/10(a), *et seq*.)
(On Behalf of Plaintiff Bishop and the Illinois Subclass)

376. Plaintiff Bishop ("Plaintiff" for the purposes of this Count) individually and on behalf of the Illinois Subclass, incorporates paragraphs 1 through 234 as if fully set forth herein.

377. The Private Information collected by Defendant from Plaintiff and Illinois Subclass Members constitutes personal information, as defined by 815 Ill. Comp. Stat § 530/5.

378. As an entity that collects, disseminates, or otherwise deals with nonpublic personal information, Defendant is a Data Collector as defined by 815 Ill. Comp. Stat § 530/5.

379. Defendant is required to give expedient notice of a Data Breach to Illinois residents whose personal information has been breached, including, Plaintiff and Illinois Subclass Members, pursuant to 815 Ill. Comp. Stat § 530/10(a).

380. By failing to give expedient notice to Plaintiff and Illinois Subclass Members, Defendant violated 815 Ill. Comp. Stat § 530/10(a).

381. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

382. As a direct and proximate result of Defendant's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff and Illinois Subclass Members have all been and continue to be harmed as a direct, foreseeable, and proximate result of Defendant's breach because Plaintiff and California Subclass Members face, now and in the future, an imminent threat of identity theft, fraud, and for ransom demands. They must now spend time, effort and money to constantly monitor their accounts and credit to surveille for any fraudulent activity.

383. Plaintiff and Illinois Subclass Members were injured and have suffered damages, as described above, from Defendant's failure to expediently notify them of the breach of their Private Information, and, therefore, seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of Defendant's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, nominal statutory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

COUNT XVII
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
(815 Ill. Comp. Stat §§ 505, *et seq*.)
(On Behalf of Plaintiff Bishop and the Illinois Subclass)

384. Plaintiff Bishop ("Plaintiff" for the purposes of this Count) individually and on behalf of the Illinois Subclass, incorporates paragraphs 1 through 234 as if fully set forth herein.

385. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

386. Defendant's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

387. Defendant's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, HIPAA, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat, and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq*, which was a direct and proximate cause

of the Data Breach;

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

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, HIPAA, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat, and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.;*

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Illinois Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, HIPAA, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat, and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*

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

389. Defendant intended to mislead Plaintiff and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

390. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that Plaintiff and Illinois Subclass Members could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

391. Defendant acted intentionally, knowingly, and maliciously to violate Illinois's

Consumer Fraud Act, and recklessly disregarded Plaintiff's and Illinois Subclass Members' rights. Numerous past data breaches in the healthcare industry and explicit warnings about data breaches put Defendant on notice that its security and privacy protections were inadequate.

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

393. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT XVIII
VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
(815 Ill. Comp. Stat §§ 510/1, *et seq*.)
(On Behalf of Plaintiff Bishop and the Illinois Subclass)

394. Plaintiff Bishop ("Plaintiff" for the purposes of this Count) individually and on behalf of the Illinois Subclass, incorporates paragraphs 1 through 234 as if fully set forth herein.

395. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

396. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

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

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

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

397. Defendant's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, HIPAA, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat, and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*, which was a direct and proximate cause of the Data Breach;

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

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, HIPAA, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat, and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*, which was a direct and proximate cause of the Data Breach;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Illinois Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, HIPAA, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat, and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*;

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

399. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

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

401. Plaintiff and Illinois Subclass Members seek all relief allowed by law, including injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying the Class as requested herein, designating Plaintiffs as Class Representatives, and appointing Plaintiffs' counsel as Class Counsel to represent the Class and Subclasses;

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

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as

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

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

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

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

JURY TRIAL DEMANDED

Plaintiffs demands a trial by jury of all claims in this Consolidated Class Action Complaint so triable.

Dated: October 8, 2024

Respectfully submitted,

By: *s/ Jean S. Martin*
Jean S. Martin
NC Bar No. 25703
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
jeanmartin@ForThePeople.com

Daniel Srourian*
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd. Suite 1710
Los Angeles, California 90010

Telephone: (213) 474-3800
daniel@slfla.com

Beena M. McDonald*
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500
bmm@chimicles.com

Counsel for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of Plaintiffs' Consolidated Class Action Complaint was filed via CM/ECF on October 8, 2024, and served on all counsel of record by way of electronic service.

Jean S. Martin
Jean S. Martin